

IT Web Security Summit 2009 Talk Summary Notes

Wire-Tap Friendly VOIP by Paul Zimmermann

PGP encryption was developed for a human rights threat model during the cold war. This culminated in a security solution, following the war, for organizations worried about sovereign states. During the 1980's USA legislation prevented strong crypto. In the past, strong crypto was seen as being a technology employed primarily by criminals. This view has, of course, changed in recent years. At the change of the century, legislature began to shift.

Today, the USA legislative environment is such that it promotes crypto. For example, medical records are to be encrypted by law. It is considered negligent, these days, if one does not use encryption, even for personal reasons. With the coming age of VOIP replacing legacy PSTN infrastructure, encryption is becoming an increasing necessity; where wire-tapping is no longer occurring at the switch, but can actually occur at the end-points. This could potentially be dangerous in large companies, due to the increased possibilities of insider trading, which could lead ultimately to black mail. Cyber crime has shifted from "harmless fun" to that which constitutes organized crime. If legislature does not enforce the encryption of VOIP traffic, due to the desire by law enforcement to be able to wire tap, then that will open the door for organized crime to also wire tap anyone, any time. The difference being, the cyber criminals are not bound by policy or even ethics.

Imagine such criminals having access to the phone calls of Prosecutors, Judges, government officials and other such high-profile individuals. This thus means that we either need to leave our telephony on the PSTN, or, if we extend to VOIP, we **need** strong crypto for the voice data.

Although this would result in a reduction in capabilities of law enforcement, there will be sufficient security benefits would vastly out-weigh the deficiency in not being able to wire-tap. However, traffic analysis is more valuable to law enforcement than raw content, whereas content – and not traffic analysis – is what criminals are more interested in. Therefore, by encrypting voice data, you inversely affect law-enforcement. An important issue is the due diligence required to be forced upon companies and organizations to encrypt their data.

An additional thought is regarding facial recognition algorithms applied to video surveillance. This has massive implications on a governmental level, as it results in a nation-wide state of Total Information Awareness. Engineers thus have a social obligation to drive such technology in the 'right' direction. Public Policy follows advances in engineering, and not the converse. Engineers therefore should steer technology in the direction of public interest.

More Money, More Problems **by Jeremiah Grossmann (White Hat Security)**

This talk focuses on the non-technical or business-logic flaws resulting in potentially large amounts of monetary loss. Business-logic flaws are not able to be scanned for or measured automatically. Which means that it is incredibly difficult to avoid and then identify, which leads to solutions being reactive, as opposed to proactive.

The following are some examples of business-logic flaws that were exploited

Coupon Codes

Mac World Free Coupons were compromised, as it was discovered that the md5 hashes of the coupon codes were “hidden” within the html.

To avoid such logic flaws, the only solution is testing, testing, and more testing.

Another coupon exploit was a case where developers left test coupon passwords in the database, which were then discovered and exploited to attain free pizzas. The lesson here is to monitor testing data.

Google Hacking

Some criminals used Google Earth for reconnaissance and sourcing materials, which can then be obtained by theft.

General

Predictable Serial Numbers. A case whereby apple's serial numbers were able to be predicted and used to collect the free replacement ipods for ipods belonging to others.

Affiliate Programs. Force Feed Cookies to a user with a particular affiliate id in case they make a purchase later on. This might be hosted on SSL as no referer information is passed on, and cannot be monitored or tracked.

Authentication without Authorization

Access to predictable URL's which are “not supposed to” be linked into the website, can be used as unfair competitive advantage. For example, could be used for trading on stocks.

Permit Systems

An example is logging or tree felling permit systems. Such systems were hacked to attain “legal” permits for the Amazon forest resulting in \$838, 000, 000.00 in a single reported incident.

The solution to business-logic flaws is to, firstly, test often, test everywhere, and secondly, detect attacks by profiling activity.

Surviving the IT Security Tsunami by Greg Day

2008 - \$1 trillion in loss due to cyber crime.
2009 Q1 - 12 million new IP zombies.
- Over 800 variants of Koobface attack.
2006 – 2007 - 246% growth in malware

Why? Money

The current trend in malware is “little and often”. This mantra results in inconspicuous activity and only identifiable when it is too late. Attackers are after the everyday person's data, not money. Data is now more valuable than cash. Trojans are on the rise, and vastly outnumber other forms of malware. Google is being used as a way to initially get access to the users via self injection attacks. Targeted Drive by websites infect resources by Cross Site Scripting attacks which might automatically download and install trojans.

Virus writers, these days, are writing trojan creation tools which are sold and supported. This allows them to instantly monetize malware without technically committing a crime. Thus, “Crime As A Service” model is becoming more and more common. A lot of sites are selling aggregated data from social networking sites. Malware is currently focusing on longevity instead of heavy malicious activity. For example, changing the system's address from which to receive system updates.

So How do we survive?

We need to employ both **REACTIONARY** as well as **PREVENTATIVE** controls. Most importantly, we need to focus on behavioural controls, such as change control, automating patch distribution and monitoring.

To optimise security we need to :

- have a common point of visibility
- translate threats into solutions
- automate security processes
- understand and utilize existing systems

CARMA – Countermeasure Aware Risk Management

In these difficult economic times, we need to integrate valuable security mechanisms to reduce manpower and increase protection.

Waiting 24 – 72 hours for protection against new threats is too long to wait for large-scale attacks. This is potentially solved via cloud-scanning; operating by comparison of meta data. This removes update times. For cases where an individual has an infection before anti-virus companies are aware, heuristics based upon report statistics combined with behavioural traits, allowing for automatic blacklisting. This allows for protection update delays decreasing from a few days to a few minutes.

Online Financial Services

by Constine G Raiu

Over 20 million malware variants now exist. Since 2008, an exponential growth has occurred. One issue resulting from this, is that it is not possible to keep up with the number of analysts to match this influx. An additional issue is the increasing complexity of the new malware. This results in increased analysis time and thus, increased response and protection times.

For example, Konficker is so complicated that no researcher is currently able to understand the malware in its totality. Thus, reactive methods are no longer viable, leaving proactive methods as the only avenue of salvation. Cyber crime surpassed drug dealing in 2006 in terms of money valuation, with an estimated value of 100 billion world wide.

Most online systems rely on a username and password combination to secure authentication, sometimes with CAPTCHA to prevent automated money transactions. This simple authentication can be easily compromised with keyloggers, password theft, phishing, social engineering. During the financial collapse, phishing criminals exploited user's fear of money loss. With the introduction of tokens, physical theft of the token device becomes an issue. In addition, trojans exist which can intercept data sent by the token and change transaction data on the fly.

Some financial institutions implement a transaction code sent via sms to verify a transaction. However, vulnerabilities exist in some mobile phone firmware which enable attackers to emulate any cell number, thus intercepting the transaction code. Another feature commonly employed is an on-screen keyboard. This is easily overcome via keyloggers which also capture screen-shots on mouse clicks.

Kaspersky Online Scanner – an online anti-virus application which scans for malware before transactions are processed. Smart Tokens are also able to avoid malware risks. However, such devices are not currently financially viable.

Kaspersky Secure Virtual Keyboard – PDM, registry guard, detection of vulnerabilities. New legislation is being employed which negates the responsibility on the bank for covering losses if the client does not employ security systems.

Cyber criminals have found ways to by-pass multi-factor authentication. The financial benefits of cyber crime is 5 x more lucrative than selling anti-malware solutions.

Bringing Cyber Criminals to Justice **by Charles Maree**

SA internet users	: 4, 590, 000
SA population	: 43, 786, 115
Police officers	: 172, 483

Cyber Crime Support is responsible for supportive / pro-active evidential intelligence operations & investigations at scenes of crime where computers are involved.

Threats can involve : Identity theft, DOS, Spam etc....

Cyber Crime Communication : Criminals use the same technologies to communicate as do normal citizens; IRC, IM, VOIP, Stenography, BBS, Newsgroups, E-Mail, PGP, P2P, TOR.

The police force brute force PGP encryption using contents of confiscated hard disks, with a high success rate.

Top Web Vulnerabilities **by Jeremiah Grossmann**

82% of websites have vulnerabilities. 63% of websites have serious vulnerabilities. 70% of most popular websites have hosted malicious content. 70% of websites have urgent issues which are not resolved.

Some of the top vulnerabilities in current websites include XSS; Information Leakage; Insufficient Authentication; SQL Injections; Predictable Resource Locations; Session Fixation; Cross-Site Request Forgery; HTTP Response Splitting; etc...

If most of a site's functionality is behind the login screen, then you lose out on "testing by the masses". Injection Attacks are most prevalent in Retail, Finance and IT industries, possibly due to legacy systems.

For web security plan :

1. What websites do I own
2. How much are they worth to me
3. Who do I want to protect from

Open Source Security For Vendors

by Window Snyder

Multi-Layered Defences is the name of the game. We need to be reactive due to financial restraints, which means if you do things right, no one notices, which then makes it difficult to justify further resources being spent on security. This often results in an initial burst at handling security, which then fizzles out.

It is important to inform users about benefits of security packages. Increased co-operation is vital for global security issues to be overcome. Open Source Community supports peer review and efficient security analysis. The more information provided by the software vendors, the better the analysis by security professionals.

With greater information available to security professionals, we can :

- Generate Security Feature Reviews
- Design with security in mind
- Have continuous security testing
- have constant availability of security updates

Book : "Threat Modelling" by Windows Snyder outlines application security review methodologies used at Microsoft.

Code reviews focus on components that directly handle user input, perform complex memory management, or perform complex parsing. A peer review process is vital. Code reviews develop a level of confidence in new code and train developers to identify common vulnerabilities.

It is crucial to involve security consultants, as they are up to date with industry standards, and possibly have seen solutions to security problems in other systems. Thus, an external consultant can give a good, unbiased review and suggestions based on the code. Auto pen testing can help speed up and increase efficiency of the security team. Not only should vendors be reacting to external vulnerability reports, but should also be actively involved in vulnerability discovery themselves.

Minor revisions and 4regular updates is much better than less-frequent, larger updates as this can greatly decrease exposure time to that vulnerability.

Cloud Computing

by Johan van der Merwe

Cloud computing might be thought of as IT outsourcing. “Software as a service”. Cloud computing means different things to different people. For example, to the CEO, he might see it as a pay-as-you go system, whereas the CIO sees cloud computing as a centralized, outsourced IT solution. With cloud computing, small companies benefit the most, as multiple entities are sharing massive hardware infrastructure. Cloud computing offers flexible scalability, hidden complexity, location-irrelevant data access.

Cloud Computing offers business agility. Businesses need to be able to modify their structure to constantly adopt to a changing consumer and legal environment. Cloud computing provides this by means of IT agility, thus allowing business processes to change easily due to flexible and scalable nature of the technology underlying cloud computing.

Cloud computing is a key component of Virtualized Enterprises in support of Business Agility.

Cloud Security Alliance : a security group governing the security of cloud computing.

Crisis in Information Security

by Adam Shostack

Due to the difficulties in quantifying the need for resources assigned to information security, it often is a challenge to function in a security-oriented way as either an engineer or a technical manager. Solving security problems, we require : observations, instrumentation, application of the scientific method (form a hypothesis and then find a method of testing it).

It is important to apply the scientific method to solving issues in information security. Possible data sources might be surveys, trade press, vulnerability data from security researchers, honeynets, experience in either an organizational or personal capacity. Some questions we need to ask ourselves are, firstly, what qualifies as “good data”, and how good is this data?

The need for data is fueled by the need to test hypotheses, and possibly disprove them. It is also used to help address key underlying questions, as to how we can improve security situations, how effective is spending versus the alternatives.

A particularly interesting source of data, is that which is produced from audits of data breaches. New legislation in America which requires disclosure of security breaches. Through the collation of the entire set of breach data – rather than individual cases – interesting trends that start developing.

Incidents are tracked at datalossdb.org

Taking incidents in isolation, however, credibility can be ascertained in support of hypotheses due to these case studies. The statistics gained show the top three incident types are “equipment theft”; “hacking”; and accidental web exposure. Thus showing the importance (and current lack) of physical security.

A recent study showed that 45% of women were willing to give away a password for a chocolate bar. This suggests that perhaps people are so overwhelmed by all the security advice that it is all being ignored.

Security economics can show information on user behaviour, nash equilibria and technology adoption, chasm crossing, insecure software (transaction costs of evaluation) etc... We can also look to spending data. One report states that companies spend more on coffee than on information security. Gordon & Loeb's 37%...

In conclusion, the way forward is to start employing the scientific method, data gathering and sharing in an effective way.

Why Bother With Security?

By Windows Snyder

A problem with information security is that you cannot determine what is vital, what matter and what we need until it becomes important and starts to matter. Thus, as an industry is, by its nature, reactive instead of proactive. Often, despite applying best practices, good is just not good enough, thus it comes down to the level of responsiveness of a security department. Although we want to have a perfect security situation, security is expensive, often this requires compromise and will never defeat a determined hacker.

Security Software is not the 'be all and end all', but does offer enough to justify cost. Yet again, we can ask ourselves "How much security is too much?" As an industry we require to make certain advances – such as defining standardised metrics – to be in a situation where we can determine a properly balanced security solution.

Moving forward, we need to capture data about success and failure, and share this data. Only through both shared data and collaboration can sufficient security metrics be defined.

Economics of Information Security

by Tyler Moore

Current security risks are made vulnerable due to lack of incentive with those in a position to implement security measures. Security is often a result of transactions between two additional parties (externality). ISP's should be pressured more into cleaning up the internet. However, due to ISP's not being directly affected by insecurities, they have little incentives to tighten up on security. This is greatly unfortunate as they are a key component in making the internet more secure. One possible solution might be to issue fixed penalties to ISP's when best practices are not applied. The value of any network increases superlinearly to its size. Switching costs also determine its value.

Shapiro-Theorem : The value of an IT company is equal to the total switching costs.

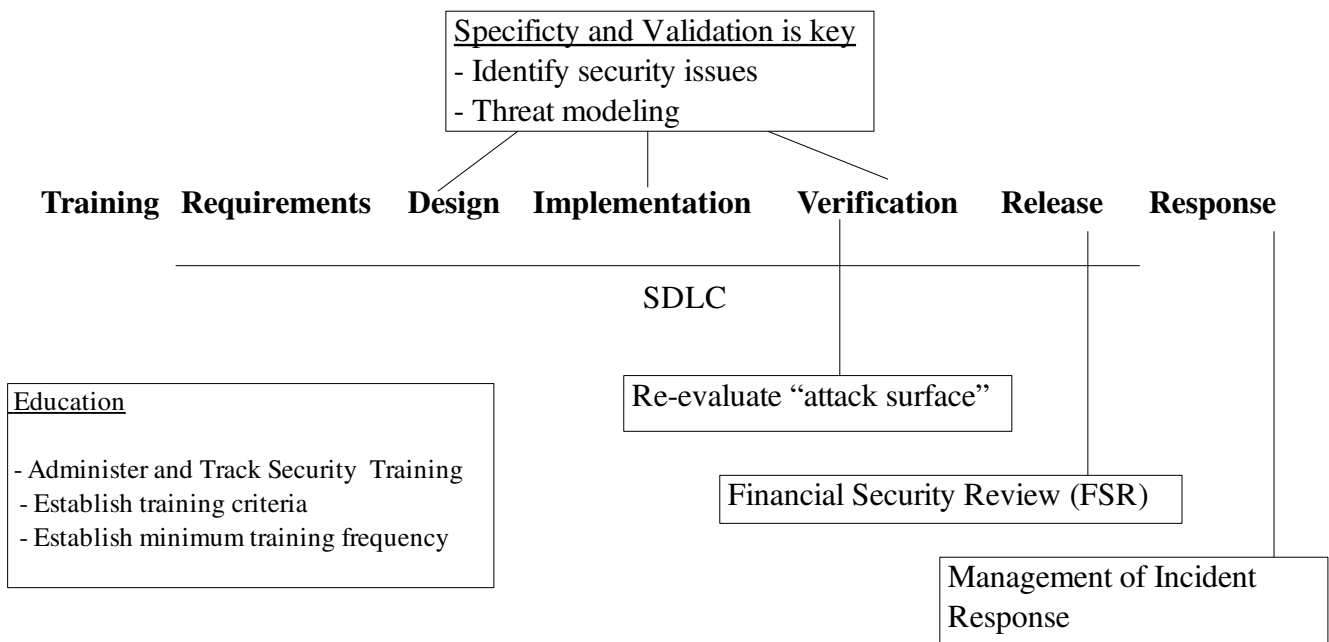
Time-to-market is a critical consideration for corporates. Research has shown that "trusting" schemes for websites is worse than ineffective, as it turns out that a site with a trusted security certificate is twice as likely to be a malicious site, as malicious sites sue this to trick users. Security should be dependant on more empirical data as to anecdotal evidence, as this leads to hype around fanciful storeys which might not lead to the development of sufficient best practices. Such empirical data could potentially come from obligatory breach reporting to guard against under reporting – which is far worse than over-reporting.

Another area where data will be useful is fraud and sabotage. Most companies find great embarrassment in releasing such figures, yet, this data would be of massive use to security researchers. An example of the effects of not sharing data is with phishing, where lists of phishing sites do not interact, causing companies and ISP's to become blind to large sets of phishing attacks, thus dramatically increasing the lifetime of the phishing sites.

Security Development Life Cycle at Microsoft

by Adam Shostack

Over the last five years, the focus of attacks has shifted from an attempt at breaking operating systems, to attacking individual systems for profit. The percentage of vulnerabilities in operating systems have halved in the last five years. Added to this, the top five software vendors are only contributing to 14% of total vulnerabilities, implying that the exploitable vulnerabilities are primarily found in smaller applications and software systems.

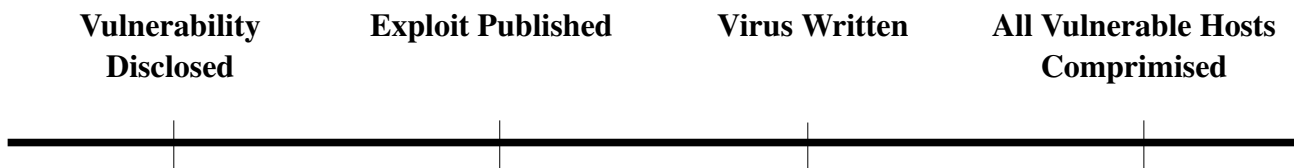


Simply looking for bugs doesn't make software secure. We need to reduce the chance for the existence of bugs. Ongoing review process is required throughout the entire life cycle.

[Http://www.microsoft.com/sdl](http://www.microsoft.com/sdl)
<http://blogs.microsoft.com/sdl>

Virtual Software Patching

by Jeroen Janssen (Tipping Point)



Most ISP's deal exclusively with signatures, with virtual software patching, a filter checks for misuse of a vulnerability. This means that protection can be applied before exploit code is published. This means that a virtual patch could potentially be released as early as 12 hours after vulnerability disclosure, and does not depend on an exploit existing for that vulnerability.

Virtual Software Patching allows for a better coverage of vulnerabilities as it is heuristic based in nature, and not signature based. This also makes it possible to protect against unknown vulnerabilities.

The false positive rate for virtual software patching is much lower due to its non-signature based nature.

[@Risk](#) weekly report by SANS

[ThreatLinQ](#) – Real-time monitoring of malicious threats

Online Privacy

by Dominic White

Due to various media discourses, there is a high degree of confusion and little agreement over the definition and importance of privacy. Today, more so than ever before, a large portion of our lives are being “lived” online. Privacy implies access control and authorized use, however it does not necessarily require the data being secretive.

Web Request

- Very basic type of information gathering.

Cross Site Tracking

- Profiling, marketing : Advertisers are required to offer opt-out processes.

Rich Browser Environments

- Tracking clipboard data, browser history, mouse clicks, etc..

Application Data

- Search requests, emails, IM chats, friend data, etc..

Aggregation, Correlation, Prediction

- Provides trends and results which initially is not obvious, psychological profile.

“Information leads to other data”, this means that although an individual leakage might seem unimportant, however, through aggregation and correlation, it can lead to a whole host of additional, more sensitive information.

Bug Hunting

by Nithen Naidoo

The space between script kiddie and hacker is ever decreasing. From analysis of data over a few years reveals that vulnerabilities are exploited up to a few months before public release. After 2006, the increased public disclosure results in decreased exploitation window. Patch management is not enough. There is a current trend in security to move away from signature detection towards anomaly detection. Custom apps and third party utilities are the logical next frontier for hackers.

Implementing Access Management in Vodacom

by Trevor Owen

One challenge facing businesses is the enormous task of securely mapping people to resources. It is important to bare in mind the gap between authorisation and access. Two primary goals exist : To give access to those who require access during the period for which they require that access, and then to keep out those who do not have access. Sub-goals include such things as privacy. Trust is an important concept which needs defining. Legitimate user access needs to be identified. Duration needs to be kept in mind, thus revoking access once the duration is up.

Barriers to access include passwords (and associated psychological issues), bureaucracy, slow provisioning, unnecessary approval processes, lack of information on authentication controls. Regarding people, not only are employees involved, but all those who potentially require access need to be considered. There needs to be validation on trust levels, establishing an identity vault, establish access policies, and automate access verification and ongoing identity validation. Another complication involves users who are shifting between different trust levels. Resource lists need to be associated with a particular role through centralized entitlement management. Entitlement associations can be used to automate access to the resource for the role.

Change management can be disrupted or cause vulnerabilities by being too automated. Barriers to authentication can be overcome by password management and customized personnel portal. Identifying and controlling back door access is crucial for continued compliance. This could be partially managed through automated auditing. A key security consideration is the revoking of both physical and system access. This could be overseen through a security steering committee comprised of upper management staff. Traditionally, only the IT department has had the power to manage authentication, however, now we are seeing a definite move towards giving human resources the ability to manage this function.

Single Sign on for applications simplifies both the user experience, as well as simplify management. Data Quality Assurance Plan ensures the quality of the integrated systems. A by-product of this system is greater visibility of user types, such as contractors. All of this is not possible without management backing.

Virtualization : Security

by Andre von Hond

Virtualization decouples the software system from hardware and offers isolation. Virtualized Infrastructure maps physical hardware to virtual machine workloads. Due to isolation and encapsulation, dynamic management of virtual machine workloads. This is primarily useful for use in data centres. VM Ware offers a new product, VSphere, which is targeted to data centres. VSphere is a VM Operating system which offers aggregation, pooling, and self healing. The V-Cloud initiative offers transparent pooling between internal and external clouds. ESX Server a hypervisor running at privilege level 0, containing the various operating systems, running at ring 1. The number one threat in any environment is misconfiguration, thus, best practices must be followed. VM Ware offer documentations, white papers and templates for compliance with best practices for implementation. Decoupling allows for introspection of virtual resources such as virtual memory and virtual CPU's, which also allows for interposition which enables greater protection against malware, due to introspection of memory and processes.

VM Safe is a set of security API's which allows for security vendors to create anti-virus software that secures multiple virtual machines. The API's were protected through certificates. Security devices, such as firewalls, can also be virtualized through the VShield product. Therefore, the entire DMZ can be virtualized and coexist on shared infrastructures. In conclusion, virtualization can be more secure than traditional systems due to isolation, introspection and inter-positioning.

Content Filtering

by Jon Hamlet

Traditional systems focus on filtering by URL's through database or cloud lookups. However, these "legacy" systems are neither real-time, nor do they sufficiently guard against dynamic content characteristics of web 2.0. Content is vulnerable to threats depending on the type of systems used to access it. Content is difficult to quantify in terms of vulnerability in real time. Another issue is the valuation of the content. Inbound threats include Web, Email, FTP, IM, P2P etc... Due to web 2.0's dynamic content, you can no longer trust sites such as Google or YouTube.

It is now becoming necessary to filter content, and not just blacklist URL's. The flow of content from internal to external systems should be carefully managed to prevent against data leakage. Content Filtering should be integrated with content flow, access control, policy controls and shared content awareness, as well as integration with threat detection and Unified hosted services. Content, context and destination awareness are all important and should ideally be integrated.

OpenSource Vulnerability Management

by Stephen Buys

Vulnerability management involves policy, monitoring, baselines, testing etc... It is necessary to define what constitutes a “known-good state”. Team members should be designated to monitoring tasks. It is also handy to monitor data from news feeds. An inventory of software enables one to understand what needs protection. Weaknesses should be discovered, versions need to be analysed, and configuration changes need to be managed and tested. Project Quant is an open source patch management project. Hardening activities include security configurations, account disablement, file permissions, stopping unused services, enable firewalls etc... Ensure quick response times, recovery and constant maintenance and documentation updates. Patch Management is just one small aspect of Vulnerability Management. Often, most systems hardening can be done by just getting the basics right, such as best practices in terms of configuring etc.... One advantage of most Open Source systems, is that they make integration between commercial systems simpler.

OCS Inventory NG – Open Source, cross platform software and hardware inventory system with remote scanning enabled.

Bastille Unix – Hardening tool for Unix based systems.

OpenVAS – Open Source vulnerability scanner with enterprise support available.

Nmap with OpenNMS or ZenMap for enumeration and host discovery.

SIGVI – Uses nmap to construct an inventory and uses that to automatically compare with NIST vulnerability database.

OSSEC – Change control with notifications, monitoring, firewall connections and root kit detection.

OSSIM – Service detection fore base-lining.

SNORT – Packet sniffing monitoring.