



One Time Passwords in DOE Computing Environments

Presented by Steve Chan sychan@lbl.gov
Network, Security and Servers Group
NERSC



Motivations



- Ongoing, widespread compromises
 - Over 20 sites that span .mil, .gov, .edu
 - Over 3000 computers
 - Unknown # of accounts
 - Specifically targeting laboratory and academic systems
 - Speculate due to the # of shared accounts
 - Very similar to unresolved compromises from 2003
- Common Modus Operandi
 - Acquire legitimate username/password via keyboard sniffers and/or trojaned clients and servers
 - Log into system and use “off the shelf” rootkits to acquire root
 - Install sniffers and compromise services, modify ssh-keys
 - Iterate
- This round of compromises, as well as the compromise from 2003 are the largest DOE compromises in recent memory (in terms of # hosts and sites)



Observations



- Users typically use the same password across many sites
 - History files provide hackers with potential remote targets
- Not possible to assure completely up to date patch levels across all systems at all sites
 - In at least one incident, kernel exploit was only published for a few weeks before it was used to gain entry
 - Kernel versions and software rev levels may not be flexible due to requirements by applications users
 - Some systems may be understaffed, or have different priorities and have trouble keeping up to date with patches
 - Some systems have are committed to vulnerable, but commonly used services (NFS)
- Bottom Line: passwords are only as secure as the least secure site that shares some of your users
- Security is an *Arms Race*
 - Hackers get smarter, and through the miracle of automation, leading edge techniques trickle down to script kiddies in a matter of months
 - There is no silver bullet, there is end in sight: we cannot afford to deploy a solution that is short sighted – must think a few moves ahead



One Time Passwords



- One Time Passwords (OTP)
 - Defangs entire class of password harvesting attacks
 - Sites that deploy OTP are now protected from vulnerabilities at other sites
 - Do not require hardware interfaces at all client systems (as SmartCards would)
 - Does not address compromised services
 - Does not address stolen long term tokens (ssh keys, grid certificates)
 - Does not address stolen short term tokens (kerberos tokens, Grid proxies)
 - If deployed without proper planning, *may* cripple:
 - Grids and Distributed Applications
 - Automated services (especially wide area automated services: file replicators)
 - **Only a single component in a broader security regime**
 - But it addresses an immediate and very damaging problem



Potential Problems



- Forcing each and every incoming connection through OTP via a single gateway
 - Bottleneck at gateway
 - Cripples bulk transfers, automated processes, distributed applications
- Users may be burdened with enormous token collection
 - Users don't like carrying around many tokens, and sometimes stop using them because they've forgotten the PIN code
- Software based tokens may not be secure
 - For convenience, soft token may be installed on laptops, cluster nodes and other locations that are vulnerable.
- If hardware tokens are shared, then must protect against cross site replay attacks
 - Time based passcodes are replayable cross site within passcode window (3 minutes in some cases)
 - Deterministic ("event based") passcode sequences subject to replay unless some form of cross site synchronization in place
 - Challenge response is safest, but some vendors do not support it (SecurID does not support CR)



Requirements (short term)



- Must have a roadmap to cross site authentication
 - Necessary to minimize the number of tokens users must carry
 - Must have provisions to prevent cross site replay attacks
 - OTP system used only for authentication, authorization is locally determined
- Must use Hardware tokens
 - s/w tokens likely to be installed on easily compromised hosts, resulting in “Emperor’s New One Time Password System”
 - Smartcards require hardware at client machines for reading – no good for mobile users
 - S/Key and OPIE are good for initial testing, but have scalability issues when it comes to managing key lists and cross site authentication
- Vendor must have demonstrated ability and willingness to support DOE Lab sized population
- Must support core services and platforms used for DOE Computing
 - Unices (Solaris, AIX, Linux, etc...)
 - Services (ssh, ftp, Grid services, Web, etc...)
 - Support RADIUS protocol, either directly or through appropriate translators
 - Support of PAM for client authentication, either directly or via radius
- Must *not* cripple
 - Bulk data transfers
 - Automated services
 - Distributed Applications and Grids



Requirements (longer term)



- Account Security is an Arms Race – so we need to think ahead
- Must be able to integrate OTP with Grids
 - Grid certs are vulnerable due to lack of password controls and inability to audit proxy generation
 - Hackers are already aware of ssh keys, minimal conceptual leap to Grid certs
 - All techniques necessary for certificate hijacking already exist
 - certs are only safe due to the relative obscurity of Grid authentication
 - A widespread move to OTP may result in requirement that proxies be issued based on OTP authentication
- Tokens such as Kerberos tickets and Grid proxies need better security
 - Kerberos vulnerabilities have been known for decades, but due to relative obscurity, it hasn't been specifically targeted
 - Grid Proxy vulnerabilities are virtually identical
 - Widespread use of Kerberos in Windows is lifting veil of obscurity
 - Once proxy certificate stolen, hackers have free access to all sites that trust that cert
 - No current method of revoking proxy certs
 - Certificate Revocation Lists do not seem to be widely enabled
 - Develop real time proxy/kerberos ticket revocation
 - Develop extensions or procedures for limiting authorization of vulnerable certs



Recommendations



- Deploy Hardware token based OTP systems that support Radius Proxies
 - Short term use of SKey/OPIE may be acceptable until federated solution becomes available, but cost of doing 2 deployments must be thought out
- Use Kerberos/GSI for bulk data transfer, automation, distributed applications and for batch jobs that need to authenticate
- Put grid certificates into a central store such as MyProxy/GridLogon
- Integrate OTP with Kerberos or MyProxy/GridLogon so that tokens can be used without dependence on static passwords
 - Deploy OCSP or related services when they become available
- Do not force a single OTP protected gateway model on users
- Investigate cross realm authentication using Kerberos and OTP
- Where possible, deploy small cross site OTP with an eye towards eventually large scale federation
- Eliminate the use ssh-keys
 - Already instances of ssh-keys being replaced by hackers, cannot be secured
- Enable and properly maintain Certificate Revocation for your site



Findings



- Current vendor provided OTP solutions are not scalable for cross site auth
 - Example: RSA SecurID supports only 6 sites (DOE alone is over 20)
 - Generally require a flat user namespace
- Tokens cannot (realistically) be shared across vendors
- Radius Proxies provide a common transport for cross site, cross vendor authentication
 - But will require routing and name translation “glue”
 - Will also need some replication strategy
- No “off the shelf” OTP solution seems to exist that will scale for cross site auth
 - vendors don’t seem interested in building such a system on our behalf
 - Home grown systems are at least a year or more away
 - Site’s plans for deployment are on much shorter time scale



Future Work



- GridLogon
- ESNet Radius Proxy fabric
- DOE labs evaluating OTP solutions
- Mailing lists:
 - otp-eng@nersc.gov : OTP engineering
 - otp-users@nersc.gov : OTP user forum
 - Send mail to majordomo@nersc.gov with
 - "subscribe otp-eng" and/or "subscribe otp-users"