Stealing Identity Management Systems

Part I: Background of Identity Management systems, and some philosiphy on attacking them

What are identity Management Systems?

- Theory of IDM
- Some specific products
- Some common configurations

Theory of IDM

- The system connecting two or more systems that hold Identities (some concept of a physical or logical user)
- Continuously manage those Identities based on a set of business rules
- Management of the identity throughout the lifecycle of the identity
  - Provisioning => Granting / Revoking privileges and changing Authentication tokens => Deprovisioning
  - All done in a way that can be proved and audited

Some specific products

- Novell Identity Manager
- Microsoft Identity Integration Server
- Sun Java System Identity Manager
- CA Identity Manager
- IBM Tivoli Identity Manager

Who's running IDM? *

- Allianz Suisse, Allied Irish Bank, Alvarado Independent School District, America First Credit Union, American National Standards Institute, Bezirk Oberbayern, Bezirk Oberbayern, Bridgepoint Health, Catholic Healthcare West, City of Peterborough, Continuum Health Partners, Coop, De Montfort University, Department of Enterprise, Trade & Employment (DETE), Deutsche Annington

* - This is just from Novell's list of succes stories: http://www.novell.com/servlet/CRS?reference_name=&-op=%25&Action=Start+Search&Submit=Start+Search&source=novl&full_text_limit=showcase_verbiage+%2C+press_release&MaxRows=0&&solutions=4&&language_id=0&region_id=0&country_id=0&industry=0

Who's running IDM?

- Eastern Michigan University, Fairchild Semiconductor, Fairfax County Public Schools, Furukawa Electric, GEHE, GKB, Gundersen Lutheran, Indiana State University, James Richardson International, JohnsonDiversey, Kanton Thurgau, Leiden University, Macmahon Holdings Ltd, Maine Medical Center, Miyazaki Prefectural Office, National Health Service (NHS), Municipality of Baerum, Nevada Department of Corrections, North Kansas City School District, Ohio Office of the Attorney General

Who's running IDM?

- Palm Beach County, Philips, Public Trust Office of New Zealand, RedSpider, Rikshospitalet, Stadtverwaltung Singen, State of Geneva, State of Nevada Welfare Division, Swisscom IT Services, The AA, Victorian Government, Waubonsee Community College

Who else?

- Search google or .gov rfp's for “identity management RFP”

What are the issues

- Complexity
- High Value
- Carelessness

Complex systems are hard to secure

- duh
- IDM systems often have a huge attack surface
  - By definition, dealing with at least 2 systems
  - Typically add in several management tools, user-facing applications and auditing systems.

High Value

- These systems almost always deal with authentication tokens (passwords, certificates, etc.)

Complacensy

- There is often a perception that as a security product, these systems are themselves secure
- Admins sometimes view “directory” information as needing little security
- Often non-intuitive to set up securely, or there are conflicting “best practices”
- For Novell systems, many have been running since before security was thought about by many admins
- To secure the system, you have to understand all of the connected systems

Many admins look at software, like Identity Manager, as a means of securing their directory, not as a liability

In summary: high complexity + high value information + carelessness = likely target for attack

Part II: Theory of the Exploitation

Leverage the Complexity

- Complexity in rapidly changing systems is usually an advantage for the attacker
- More systems = more unique vulnerabilities will discovered
- Defender has to deal with change management bureaucracy

“Hot” technology often has poor code quality as companies rush to implement

IDM systems can be attack at the...

- Network Layer
  - IDM system usually connects systems over a network
- Connected System layer
  - directories, databases, OS authentication mechanisms, etc.
- Application Layer
  - IDM application, system agents, and management tools
- Rules
  - The chosen business rules can often be exploited
- Rules
  - implementation of rules and the programmatic processing can often be exploited

Part III: Novell Identity Manager

Why am I presenting this stuff?

- Novell has made several security architecture decisions that I think are bad, and they are not clearly explained to many customers
- Even when security best-practices are followed, vulnerabilities can still be exploited
- I would like to see these problems addressed

A minimal Novell system

- eDir
- Metadirectory Engine
- Drivers (usually from Novell)
- Driver ruleset

Some Typical Novell Configurations

Security Best Practices

(from the 3.0.1 Administration Guide)

- Use SSL
  - Engine to Remote Loader
  - Engine or Remote Loader to application
- Monitor and Control access to: Driver sets, Drivers, Driver configuration objects (filters, style sheets, policies), Password policy objects (and the iManager task for editing them)
- Don't allow too much information in Password Hint attributes

Security Best Practices (cont)

- Force password changes after admin resets
- Create Strong Password Policies
  - So by implication, use Universal Passwords
- Secure Connected Systems
- “Follow industry best practices for security measures, such as blocking unused ports on the server.”

Security Best Practices (cont)

- Various Designer Recommendations
  - Limit Consultants rights
  - Control .proj files
  - delete log files
  - Secure connection from Designer to directory
  - Don't use encrypted attributes
  - Don't store passwords that are sensitive

Security Best Practices (cont)

- Tracking Changes to Sensitive Information
  - Done with Novell Audit
  - Recommended operations to log: Change Password, Password Set, Password Sync, and Driver Activity

Part IV: Exploitation

Goals of Exploitation

- What are the targets when attacking an identity management system?
  - Gain access in connected system
  - Exceed authorization in a system
  - Steal someone's identity in a system (control authentication tokens)
  - Break the auditing

Exploitation Targets

- Exploits in the IDM system components

Exploitation Targets (2)

- Modify the IDM system

Exploitation Targets (3)

- Use the system rules to your advantage

Exploitation Targets (4)

- Exploit the rules processing

Exploitation Targets (5)

- Exploit the remote loader, and connection to the remote loader

Exploitation Targets (6)

- Passwords
  - Windows Passwords
  - Universal Passwords

Exploitation Targets (7)

- Auditing subsystem

Conclusions