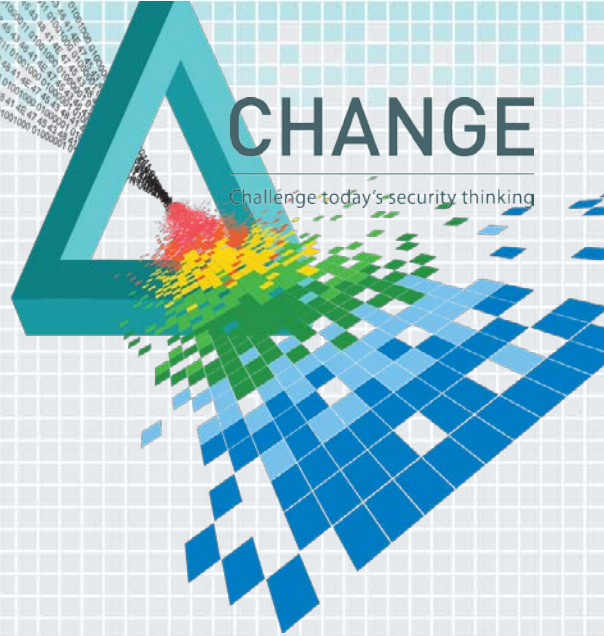
RSA Conference2015
San Francisco | April 20-24 | Moscone Center



SESSION ID: HTA-R03

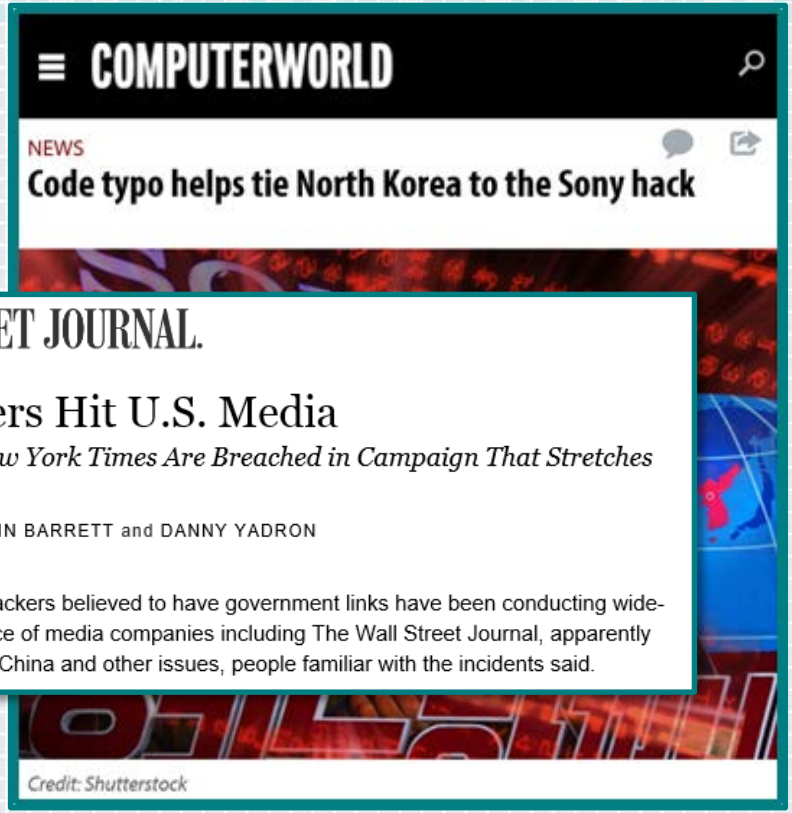
Pass-the-Hash II: The Wrath of Hardware

Nathan Ide

Principal Software Engineering Lead
Microsoft, Windows security

Pop Quiz, Hot Shot

- Which would you stop:
  - Largest bank heist in history
  - Theft of customer PII
  - Politically-motivated hacking



THE WALL STREET JOURNAL.

MEDIA & MARKETING

Chinese Hackers Hit U.S. Media

Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Several Years

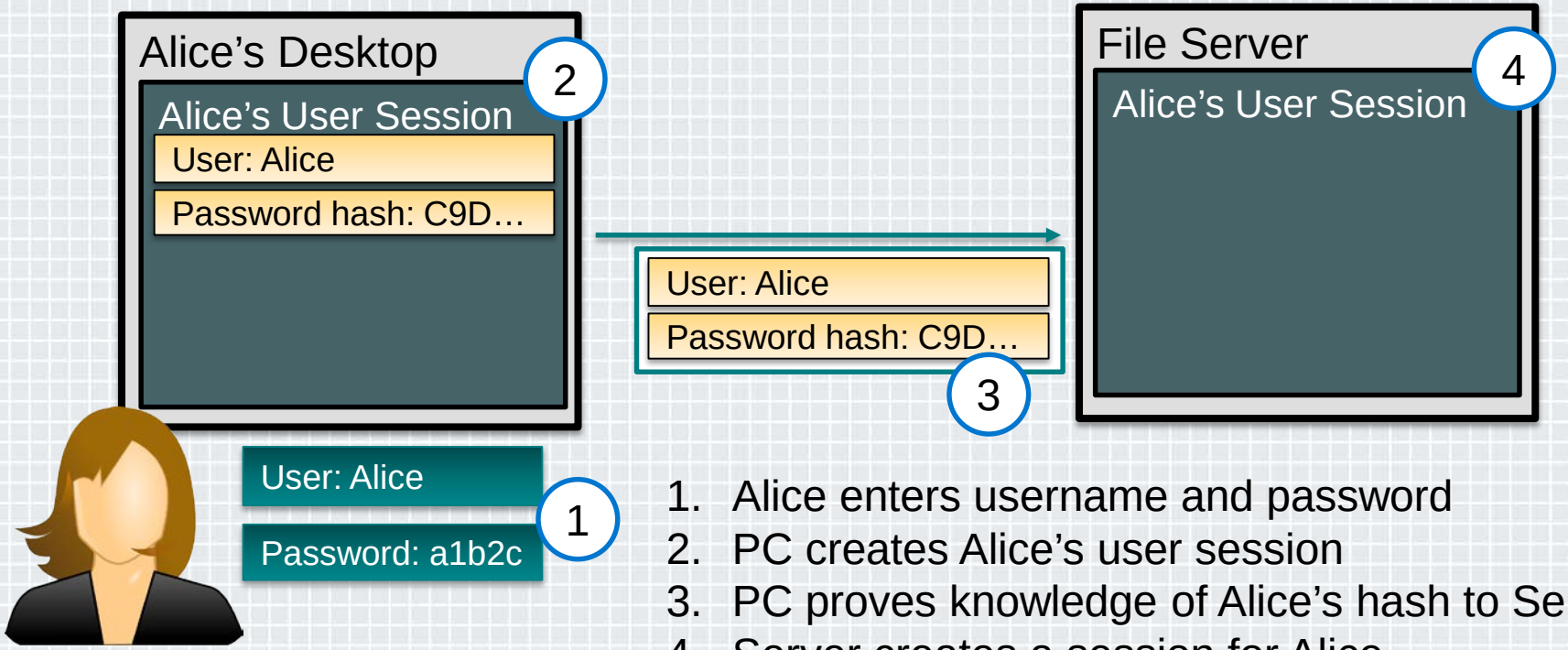
By SIOBHAN GORMAN, DEVLIN BARRETT and DANNY YADRON

Updated Jan. 31, 2013 8:28 p.m. ET

WASHINGTON—Chinese hackers believed to have government links have been conducting wide-ranging electronic surveillance of media companies including The Wall Street Journal, apparently to spy on reporters covering China and other issues, people familiar with the incidents said.

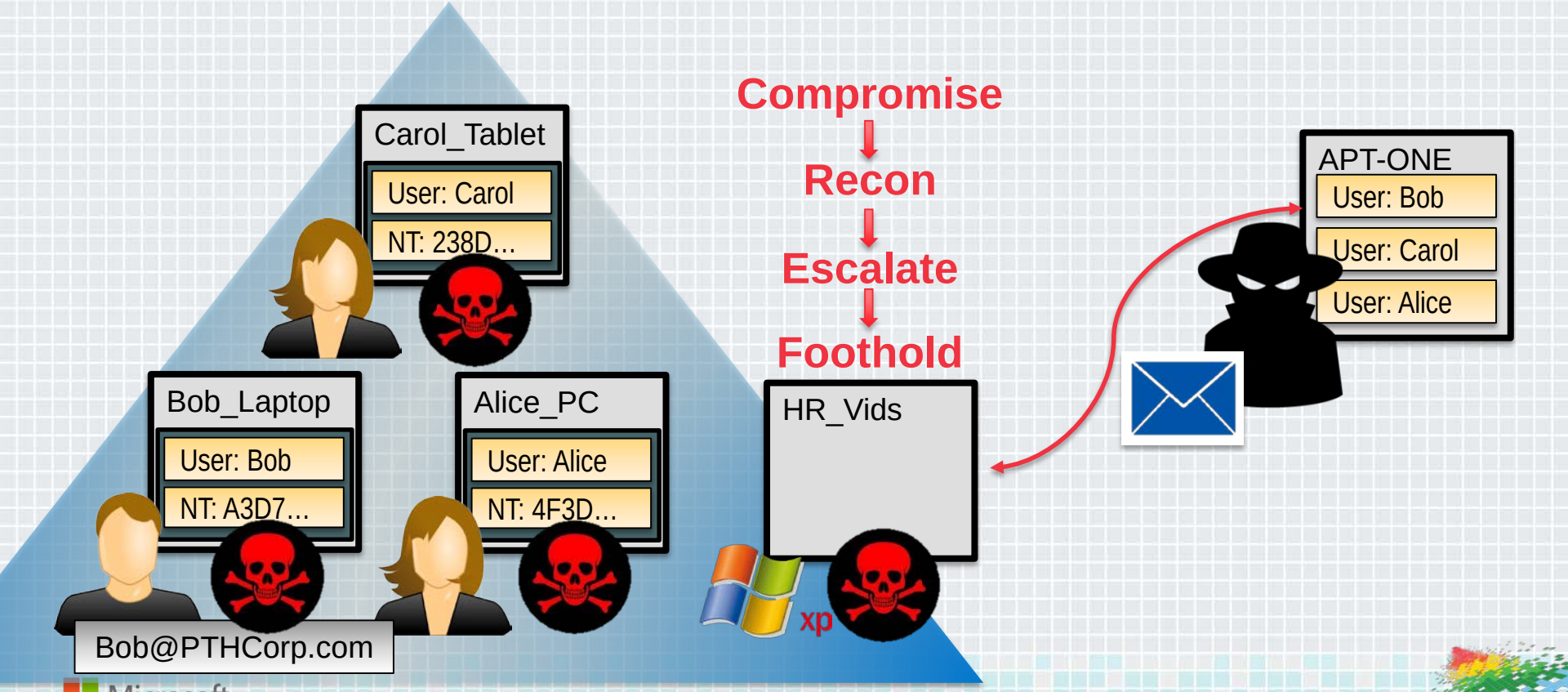
- Good news! You don't need to choose. All exploit **AD Single Sign-On** (SSO)

Single-Sign On, Explained



1. Alice enters username and password
2. PC creates Alice's user session
3. PC proves knowledge of Alice's hash to Server
4. Server creates a session for Alice

Pass-the-Hash Technique



The Future! (if you can get there)

- New protocols learn from these attacks

Token Binding (tokbind)

Documents | **Charter** | History | Dependency Graph

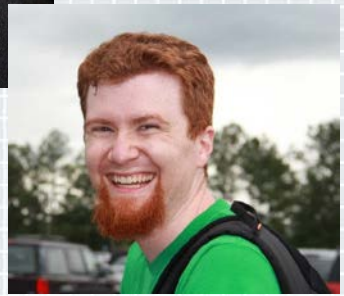
Charter for Working Group

Web services generate various security tokens (e.g. HTTP cookies, OAuth tokens, etc.) for web applications to access protected resources. Currently these are bearer tokens, i.e. any party in possession of such token gains access to the protected resource. Attackers export bearer tokens

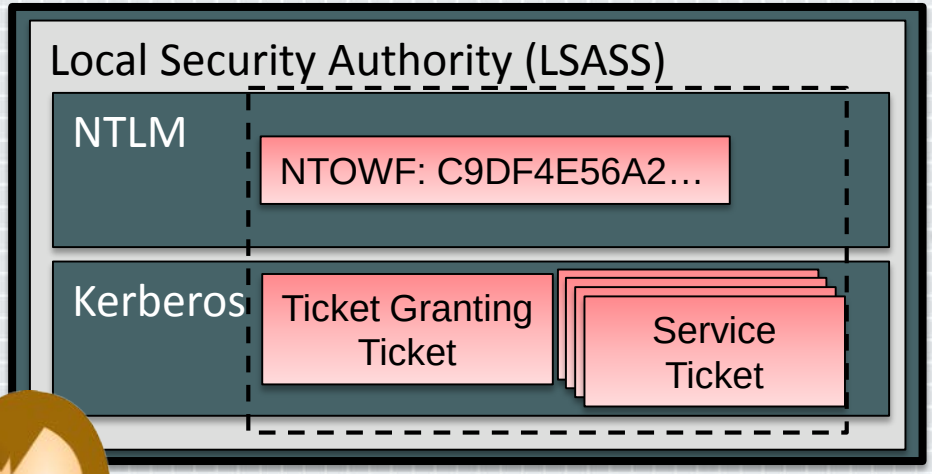
- NAS, printers, software, hardware rely on NTLM & Kerberos
- *Security or compatibility, choose one*
- **Unless …**

Bringing new security promises to old protocols

Physical Token Theft



Digital Token Theft



"Credential footprint"

Token Theft - Demo

Current Defenses

- Binding to devices with silos/policies
  - Theft still possible on restricted machines
- Reduced credential footprint
  - SSO means attacker still has something to steal
- Process/Kernel code signing
  - Eliminates polymorphism, but requires A/V signatures

Servicing frequency & definition of “Old”

Monthly | <3 Years | 5 Years | >5 Years

OS Patches

Client Devices

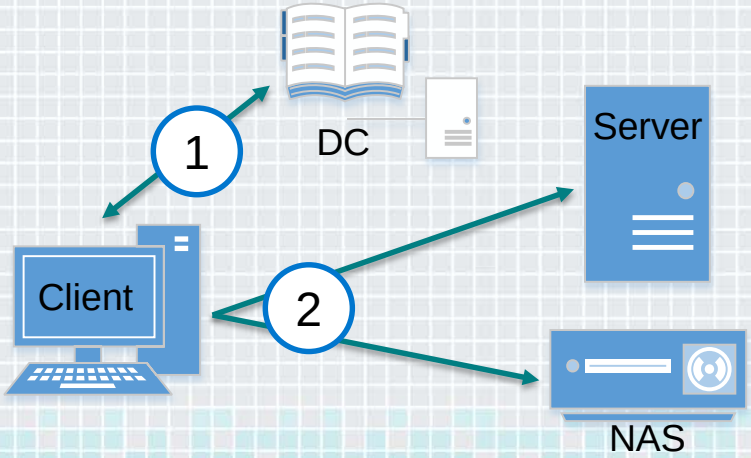
Domain Controller

Servers

LOB tools

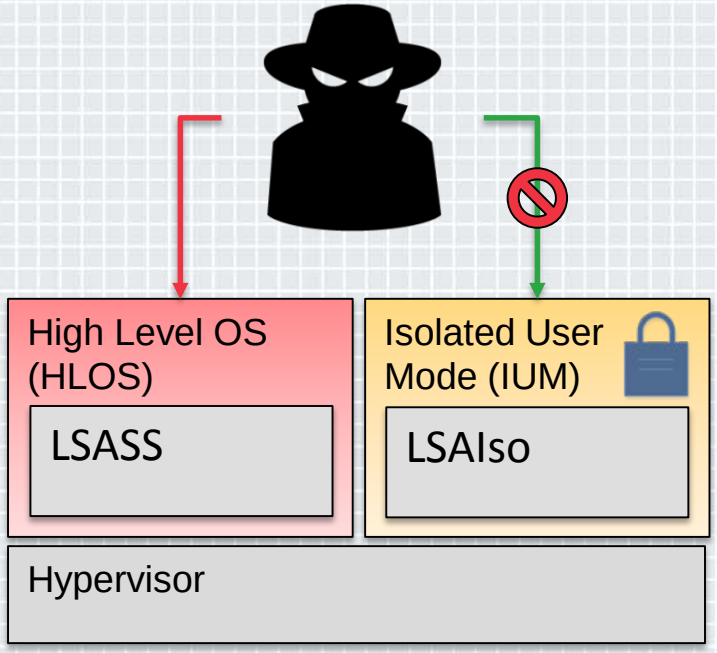
ACLs

Appliances



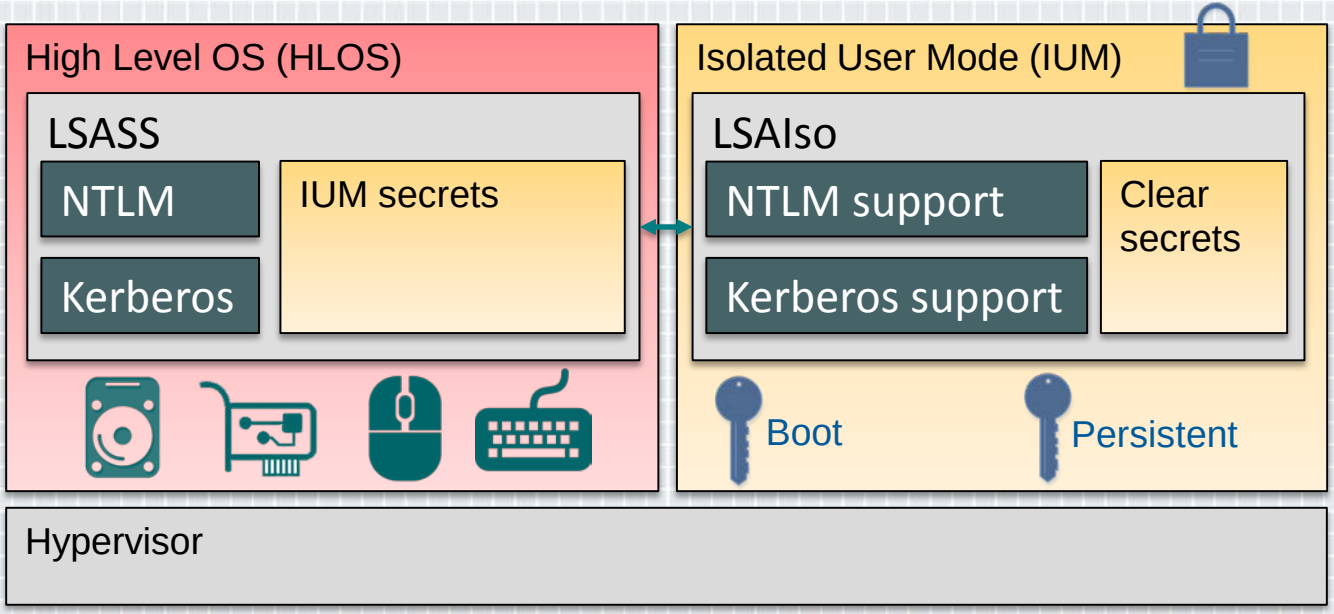
New technique

- Use hardware virtualization
  - “Isolated User Mode” (IUM) provides strong isolation boundary
  - Strict signing - doesn’t host device drivers
  - Building block for all security promises

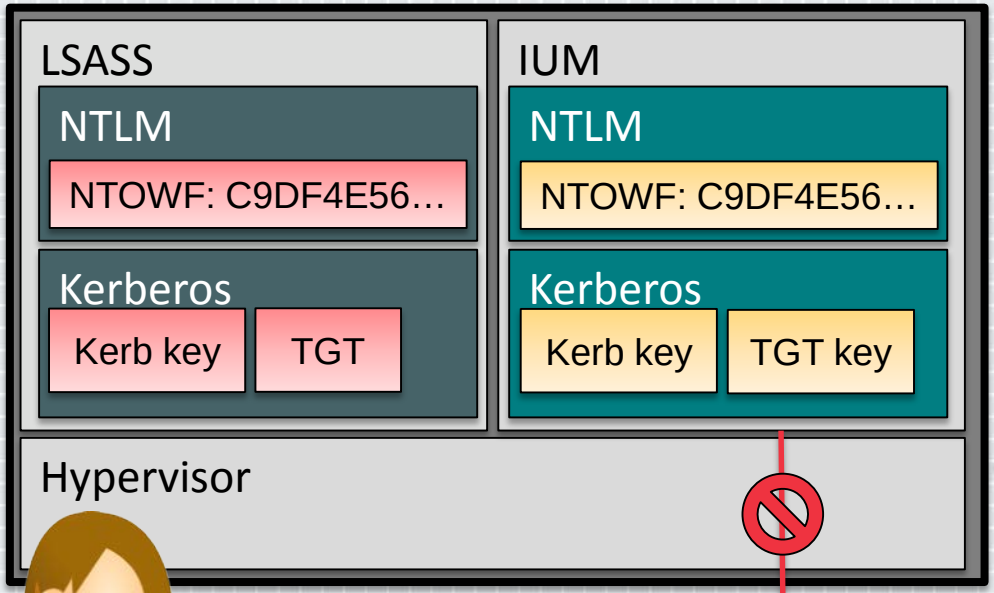


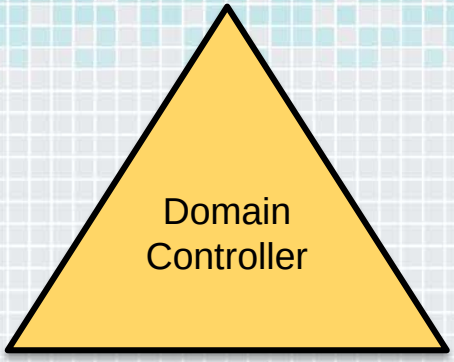
10,000’ Architecture

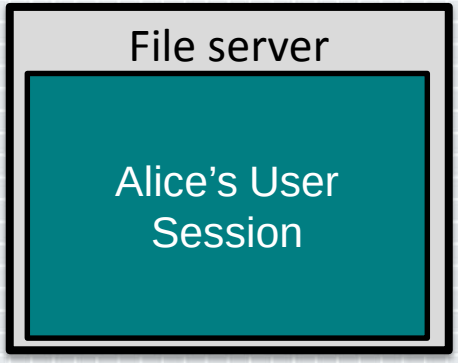
- Windows 10 has IUM with builtin NTLM and Kerberos support



IUM login flow



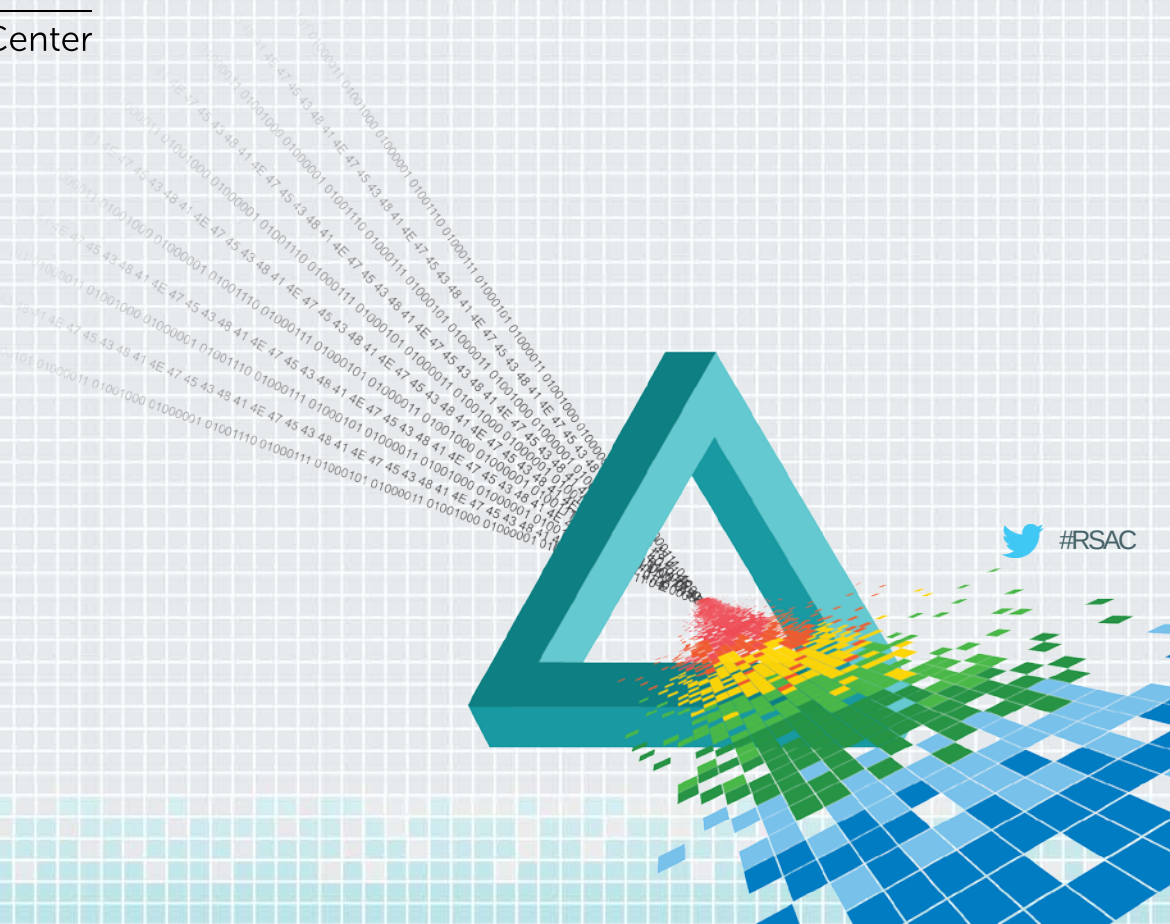




User: Alice

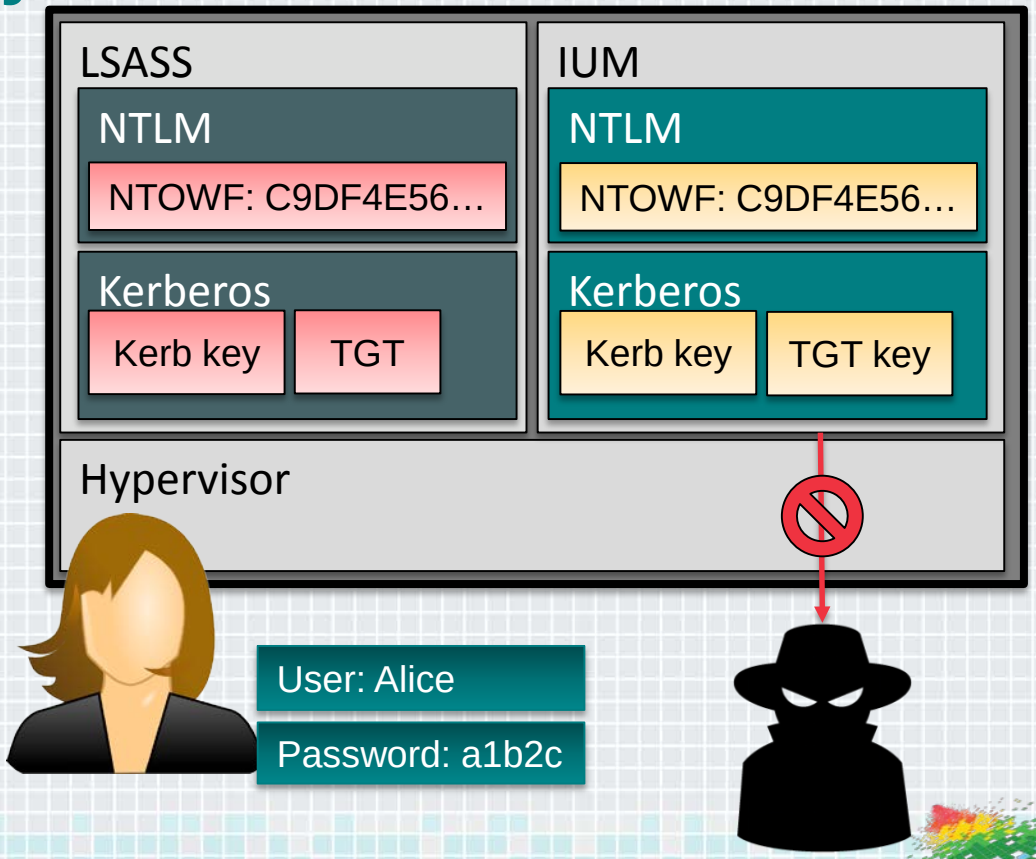
Password: a1b2c

IUM - Demo



Cred Theft Law of Physics #1

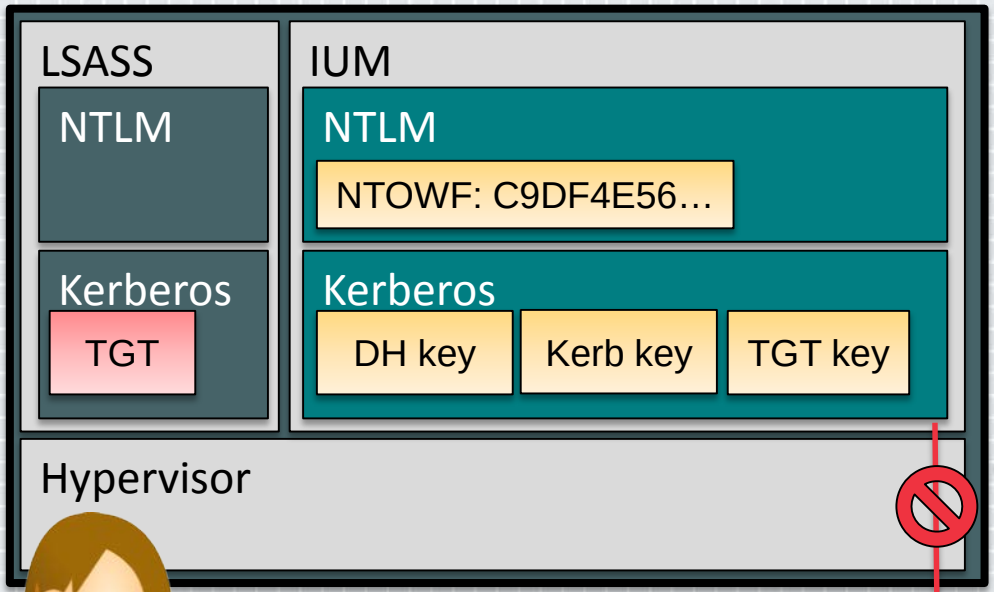
- Credential theft begins with hostile administrator
- If user credential comes from keyboard, it's compromised

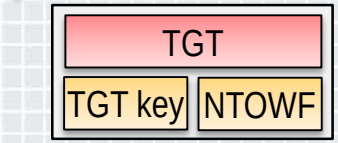


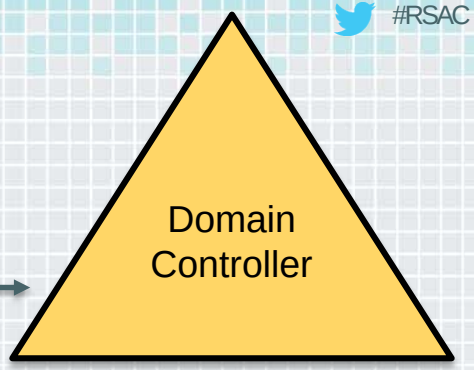
Strong cred support in NTLM, Kerberos

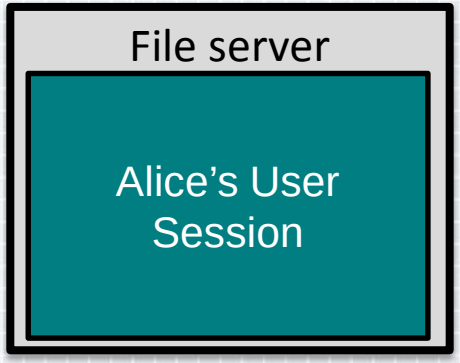
- Symmetric secret auth used to be “good enough”
- Hardware bound asymmetric auth stops phishing
  - In AD since Win2000
  - Uses PKINIT Kerberos extension
  - Supports Diffie-Hellman key exchange
- But, NTLM password based protocol!
  - DC sends you hash

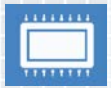
IUM Smartcard integration











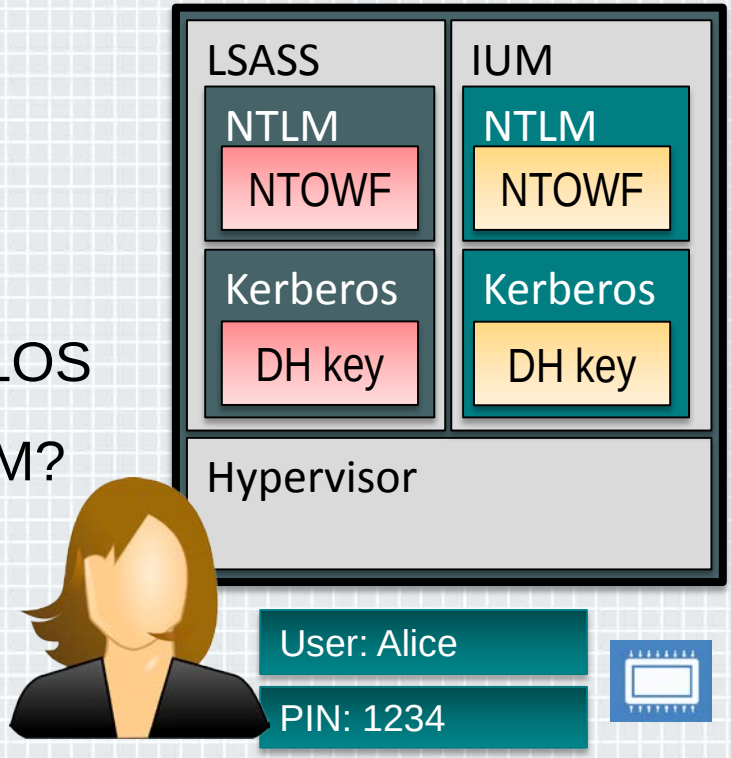
RSAConference2015

San Francisco | April 20-24 | Moscone Center

Smartcard authentication in IUM - Demo

Cred Theft Law of Physics #2

- Costs favor attacker
  - Shipping is expensive
  - Deploying is expensive
- Devices owned by (compromised) HLOS
- What forces the Smartcard to use IUM?
- Need to bind user accounts to IUM!



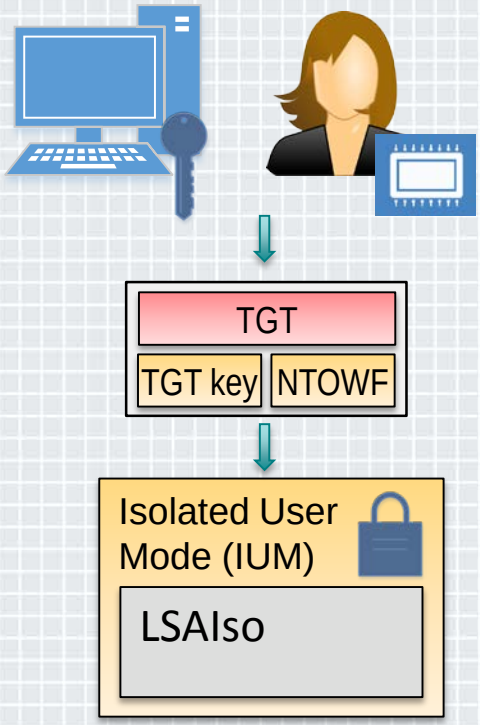
IUM Credential Binding - Demo

Attacking IUM

- Extraction is not the only way to get data
- IUM is oracle
  - Susceptible to sidechannel and brute force attacks
  - Must restrict oracle crypto
- MS-CHAPv2, NTLMv1 *blocked*
- Smartcards restricted to DHE exchange
- New trust boundary – firmware, IUM, hardware

Putting it together …

- IUM-bound machine key …
- Armors hardware-bound user key …
- Retrieves TGT and encrypted NTLM hash …
- Decrypted in IUM
- **NTLM SSO without extractable NTLM hash!**



Apply

- Hardware-backed credential theft defenses don't require starting over
  - Eliminate weak protocols – MSCHAPv2, NTLMv1
  - Migrate users to hardware credentials
  - Update hardware and software specs to IUM-compatible devices
    - You can try demos at home with the Win10 April preview ☺
- Get educated on other Credential Theft mitigations
  - http://www.microsoft.com/pth