

RESTENA CSIRT



TF-CSIRT Seminar

17 sept 2010

Tracing individual users in IEEE 802.1X networks

Stefan Winter <stefan.winter@restena.lu>

Introduction



- IEEE 802.1X networks
 - Example: eduroam
- Linking offending IP address to authenticated entity
 - IP -> MAC
 - MAC -> Outer identity
 - Outer identity -> Inner identity
- Requirements on operators
- Interfacing with CSIRTs

IEEE 802.1X networks



- Provide IP layer connectivity only to authenticated entities (“known users”)
- Authentication on layer 2
 - Support for credential encryption
 - Support for identity privacy
 - On wireless networks: per-user encryption
- Can be used to provide roaming support (transitive trust between operators)
 - Nice...
 - ...but involves many parties (and thus provides ample room for human error)

Example:



- ~ 1000 hotspots (mostly universities) in Europe and beyond deploy IEEE 802.1X
 - Under common branding: “eduroam”
 - Backend RADIUS infrastructure provides roaming support: user from university A can roam at hotspot of university B
 - Users log in with “`local_id@uni-a.xy`”
 - Credential management always with home university (eduroam enforces mutual auth with EAP)
 - IP access always with hotspot
- Several million registered users

What's the deal with “identity privacy”?



■ Roaming

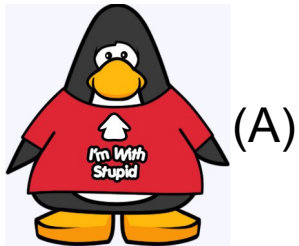
- ❑ requires hint to reach home server - “@uni-a.xy”
- ❑ Does **not** necessarily require local_id
- ❑ User can use `anonymous@uni-a.xy` for routing purposes, but `local_id@uni-a.xy` for authentication purposes
- ❑ User can use `don.stikvoort@uni-a.xy` for routing purposes, but `local_id@uni-a.xy` for authentication purposes

■ Non-roaming case:

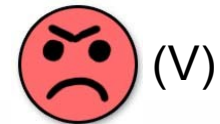
- ❑ Communication steps on following slides collapse into easier model
- ❑ But user can still obfuscate, admin needs to check carefully!

■ Hotspot does not see local_id!

Attack scenario



Ronald Duck
ronald@dismay.com



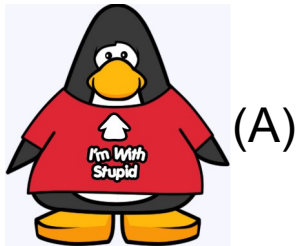
attacked from IP
198.51.100.23

- somewhere on the internet, V is attacked by a IP address
- somewhere else on the internet, A is responsible for this attack
- linking from IPv4(A) to A involves work!

Attack scenario (CSIRT)



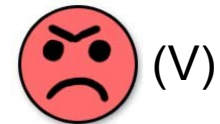
attacker's home domain



Ronald Duck
ronald@dismay.com

hotspot

victim



attacked from IP
198.51.100.23

↓ informs

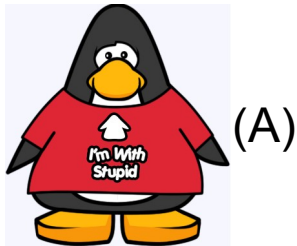


- user informs his own CSIRT(V) [Info: timestamp; attacker IP]
- CSIRT(V) informs CSIRT(H) with [Info: timestamp; attacker IP]

Attack scenario (hotspot)



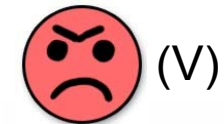
attacker's home domain



Ronald Duck
ronald@dismay.com

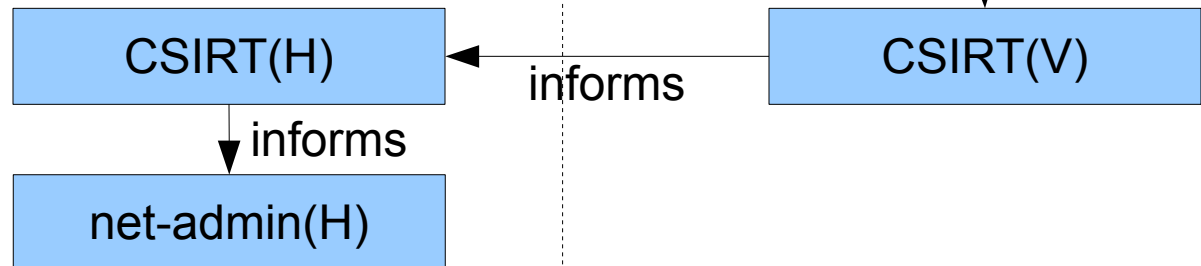
hotspot

victim



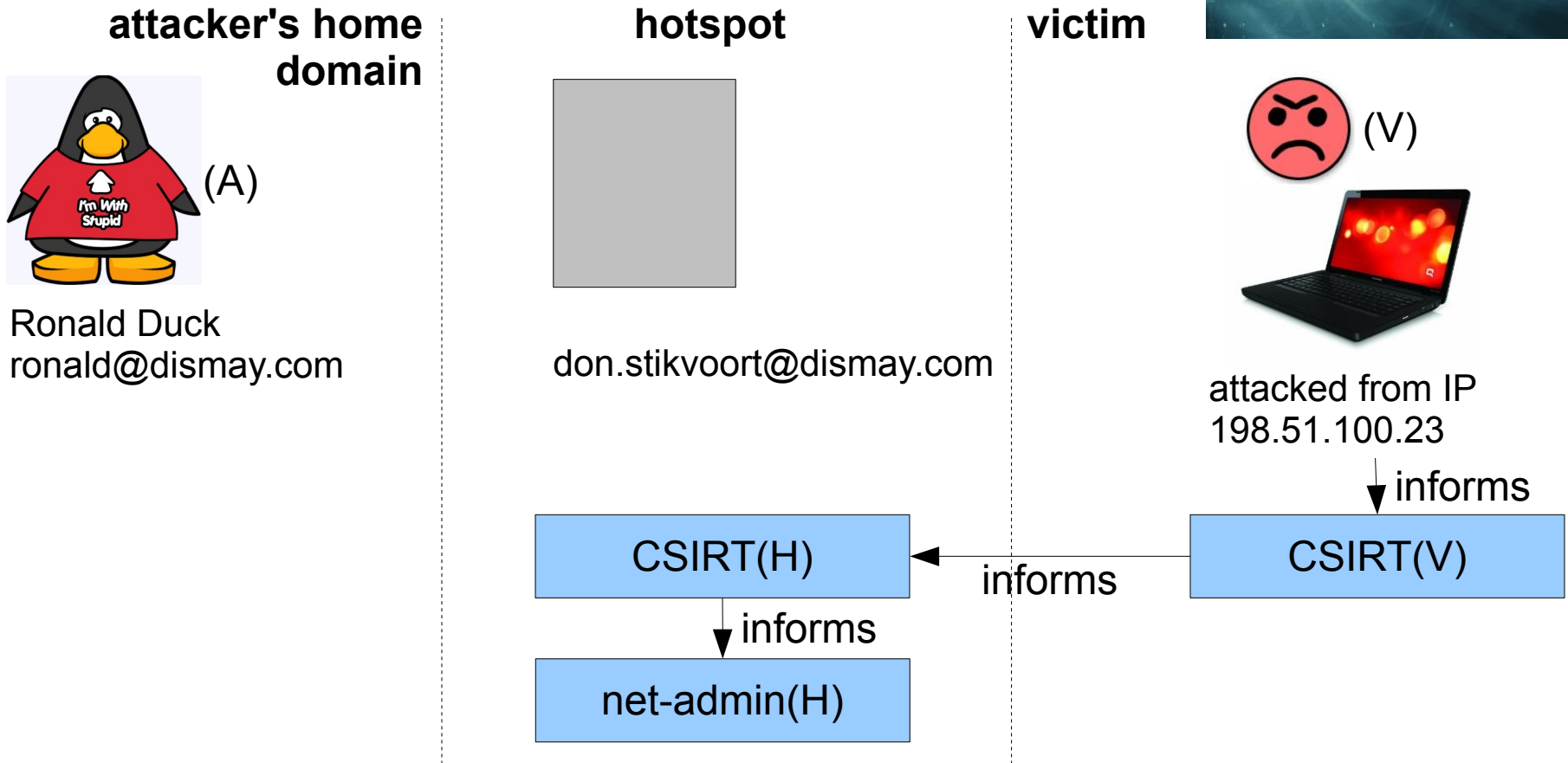
attacked from IP
198.51.100.23

↓ informs



- CSIRT(H) looks up subnet, finds responsible network admin
- informs net-admin(H) with [Info: timestamp; attacker IP]

Attack scenario (hotspot, 2)



- net-admin(H) links attacker IP at timestamp to attacker MAC address (DHCP logs, ARP sniffing, cursed be NAT)
- checks authentication logs to bind MAC to outer identity

Hotspot: logs



14:45:36 : [WLAN-1] Associated WLAN station 00:13:ca:c2:b1:86 (Intel-Corporate c2:b1:86)

14:45:36: [WLAN-1] WLAN station 00:13:ca:c2:b1:86 (Intel-Corporate c2:b1:86) authenticated via 802.1x [user name is don.stikvoort@dismay.com]

14:45:36: [WLAN-1] Key handshake with peer 00:13:ca:c2:b1:86 (Intel-Corporate c2:b1:86) successfully completed

14:45:36: [WLAN-1] Connected WLAN station 00:13:ca:c2:b1:86 (Intel-Corporate c2:b1:86)

14:45:43 : [WLAN-1] Determined IP address for station 00:13:ca:c2:b1:86 (Intel-Corporate c2:b1:86) [ap-2.rest]: 158.64.3.35

Hotspot: logs (2)

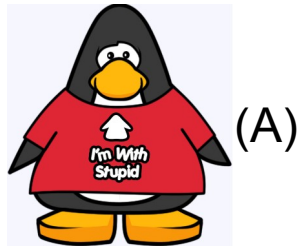


- **Request** (Fri May 2 14:45:36 2008)
Packet-Type = Access-Request
User-Name = "don.stikvoort@dismay.com"
NAS-IP-Address = 158.64.3.2
Calling-Station-Id = "00-13-CA-C2-B1-86"
NAS-Identifier = "ap-2.rest"
EAP-Message = 0x0201 6c75
Message-Authenticator = 0x9395 cd71
Realm = "restena.lu"
Proxy-State = 0x313935
- **Accept** (Fri May 2 14:45:36 2008)
Packet-Type = Access-Accept
MS-MPPE-Recv-Key = 0x9737 ae97
MS-MPPE-Send-Key = 0x78e3 aad8
EAP-Message = 0x03070004
Message-Authenticator = 0x8949 729a
Proxy-State = 0x313337

Attack scenario (hotspot, 3)



attacker's home domain



Ronald Duck
ronald@dismay.com

hotspot



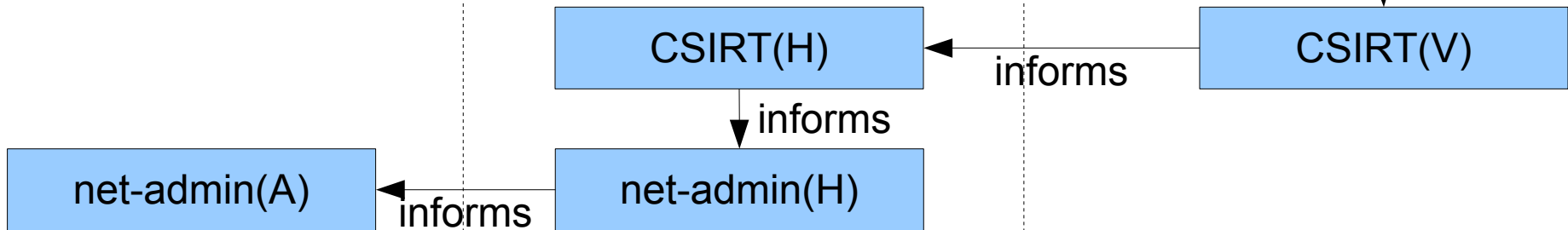
don.stikvoort@dismay.com

victim



attacked from IP
198.51.100.23

↓ informs

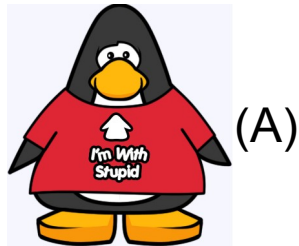


- net-admin(H) needs to find out responsible admin for @dismay.com
- informs net-admin(A) with [Info: MAC, outer id, **authentication** timestamp]

Attack scenario (home server)



attacker's home domain



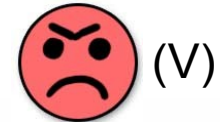
Ronald Duck
ronald@dismay.com

hotspot



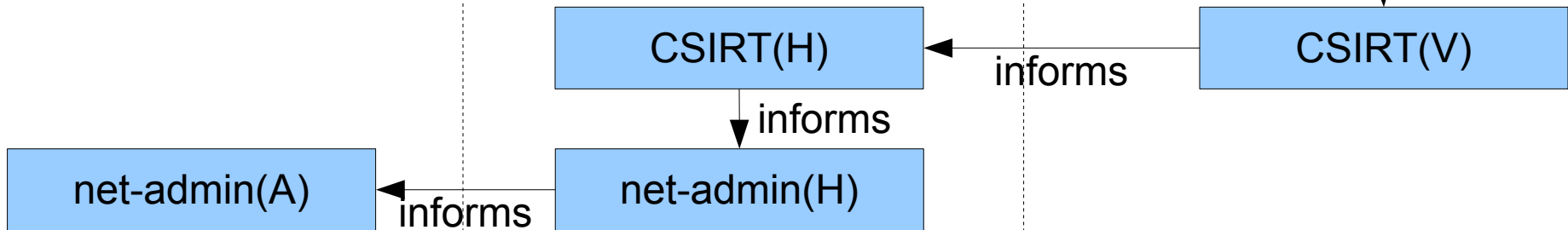
don.stikvoort@dismay.com

victim



attacked from IP
198.51.100.23

↓ informs



- net-admin(A) checks authentication logs of the authentication in question
- finds out that attacker id is ronald@dismay.com
- can take appropriate measures of punishment for **Ronald Duck**

Home server: logs



- **Only** visible for home server (TLS tunnel spans between connecting device and home server)
- **Request** (Fri May 2 14:45:36 2008)
User-Name = "ronald.duck@dismay.com"
User-Password = "hahatooeasy"
FreeRADIUS-Proxied-To = 127.0.0.1
- **Accept** (Fri May 2 14:45:36 2008)
Packet-Type = Access-Accept

An Alternate Reality



- net-admin(H) could report to CSIRT(H) instead
 - CSIRT(H) is told/finds out about home server in question
 - CSIRT(H) finds responsible CSIRT(A)
 - CSIRT(A) contacts net-admin(A)
- Advantage
 - Gets CSIRT(A) into the loop
 - Keeps CSIRTs in the loop at all times
- Disadvantage
 - CSIRT(H) needs access to operator DB

Requirements on Operators



■ Hotspot

- ❑ Keep authentication logs (RADIUS et. al.)
 - Auth logs must contain MAC address
- ❑ Keep IP -> MAC binding logs (open question: IPv6 privacy extensions)
- ❑ Synchronised time!

■ Home Server

- ❑ Keep authentication logs (RADIUS et. al.)
- ❑ Maintain user db for binding to an individual
- ❑ Synchronised time!

Interfacing with CSIRTs



- Which path is preferred?
 - i.e. handle via CSIRT(H), and let net-admins “do their stuff”
 - or involve CSIRT(A)
- For eduroam, we simply (simplisticly?) state:
 - “Whenever necessary and appropriate, incidents should be handled by the respective CERT(s).”
 - That can be refined for next iteration of “eduroam Service Definition”
 - We are open for suggestions!



The End.