

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



**Análisis de protocolos de
seguridad criptográficos
utilizando métodos y
herramientas simbólicas**



- Santiago Escobar Román
- Titular de Universidad
Universitat Politècnica de València (UPV)
- sescobar@dsiv.upv.es



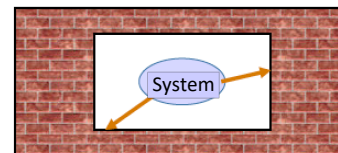
Índice

1. Safety & Security
2. Protocolo TLS 1.3
3. API Yubikey & YubiHSM
4. Maude-NPA protocol analyzer



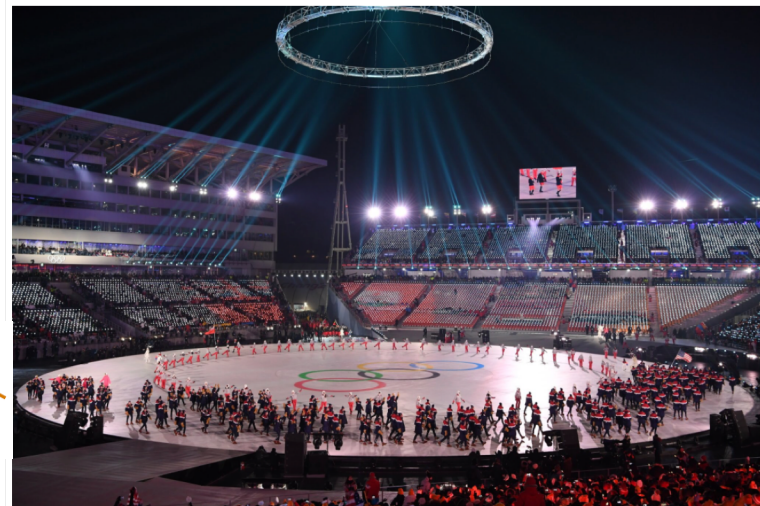
Safety (Inofensivo)

Libre de pérdidas o accidentes



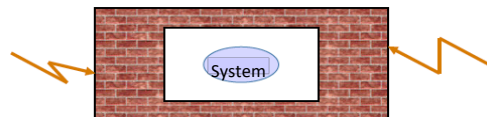
Cyberattack Caused Olympic Opening Ceremony Disruption

By NICOLE PERLROTH FEB. 12, 2018



Security (Seguro)

Protección contra ataques





- ¿Qué es la seguridad?
 - Todos queremos tener sistemas seguros (safety & security)
 - Pocas personas definen qué es exactamente, ni siquiera vagamente.
 - Confidencialidad, integridad, disponibilidad (CIA).
- Seguridad en la red
 - Proteger la infraestructura de redes, routers, switches y servidores de dominio.
 - Múltiples capas de defensa, cada una con sus políticas y controles.
 - Controles de acceso, malware, firewalls, web security.
- Seguridad Informática (IT Security)
 - Protegiendo sistemas que manejan datos sobre ciudadanos, corporaciones, gobiernos, etc.
 - Evaluando requisitos, políticas, mecanismos y componentes.
- Seguridad de la información
 - Accesos no autorizados, divulgación, interrupción, modificación o eliminación de los datos.
- Ciberseguridad
 - Protegiendo datos en formato electrónico. Sistemas ciberfísicos (entornos industriales)
- Security by Design (Diseño Seguro)
 - Ingeniería Software. Seguridad demostrable. Criptografía. **Protocolos de seguridad**



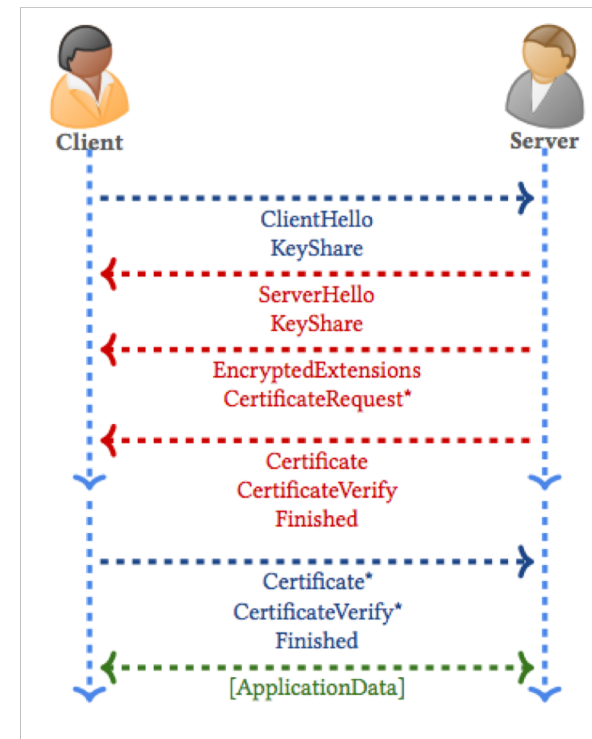
Índice

1. Safety & Security
2. **Protocolo TLS 1.3**
3. API Yubikey & YubiHSM
4. Maude-NPA protocol analyzer



Protocolo TLS

- El protocolo criptográfico “**Transport Layer Security**” (**TLS**) ha prometido ser más seguro, veloz y privado que su predecesor SSL
- Aplicaciones web actuales siempre usan una web segura.
- HTTP da el paso a HTTPS, siendo el protocolo de seguridad TLS el responsable actualmente.
- Los navegadores más importantes (p.ej. Google Chrome) dan el paso a mayor seguridad para sus usuarios





Protocolo TLS

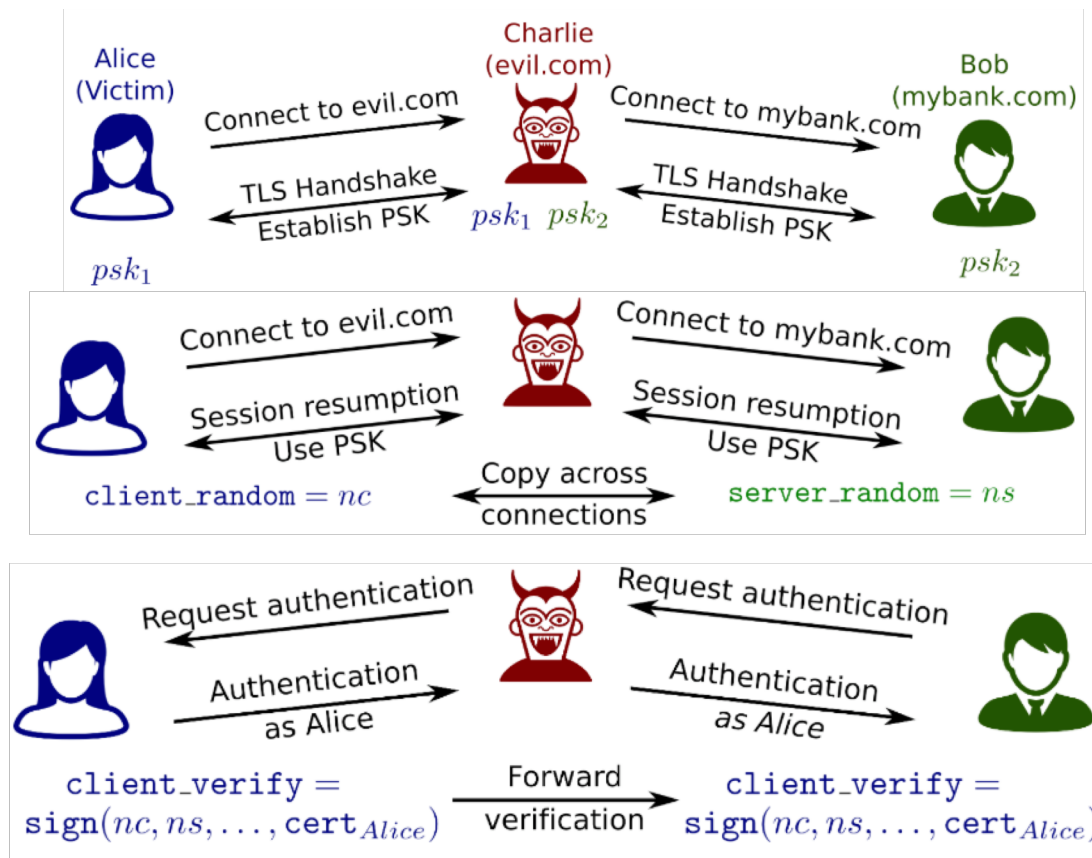
- “Internet Engineering Task Force” (IETF) define las distintas versiones
 - TLS 1.0 definido en Enero 1999 en RFC 2246
 - TLS 1.1 definido en Abril 2006 en RFC 4346
 - TLS 1.2 definido en Agosto 2008 en RFC 5246
 - TLS 1.3 definido en Agosto 2018 en RFC 8446
- La versión TLS 1.2 tiene un ataque (CVE-2015-7575)
 - Security Losses from Obsolete and Truncated Transcript Hashes (SLOTH)
- IETF decide seguir una aproximación “**Analysis-before-deployment**” en para TLS 1.3
 - Se han encontrado varios ataques y problemas durante el diseño de TLS 1.3



Protocolo TLS

- Draft versión 10 TLS 1.3
 - Equipo de investigación compuesto por University of Oxford & University of London
 - Uso de la herramienta Tamarin prover (ETH Zurich)
 - Man-in-the-middle attack
 - “Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication”
2016 IEEE Symposium on Security and Privacy
- Draft versión 21 TLS 1.3
 - Mismo equipo de University of Oxford & University of London
 - Verifican ataque versión 10 está resuelto
 - Detectan nuevos fallos de autenticación
 - “A Comprehensive Symbolic Analysis of TLS 1.3”
2017 ACM SIGSAC Conference on Computer and Communications Security

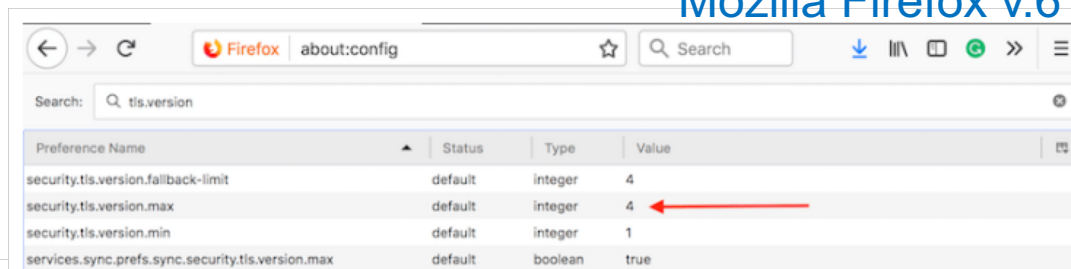
Protocolo TLS



Protocolo TLS

- TLS 1.3 se encuentra en nuestros navegadores desde octubre del 2018

Mozilla Firefox v.61



Google Chrome v.63

TLS 1.3

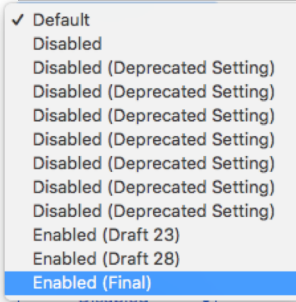
Sets the TLS 1.3 variant used. – Mac, Windows, Linux, Chrome OS, Android
[#tls13-variant](#)

Scroll Anchor Serialization

Save the scroll anchor and use it to restore the scroll position when navigating. – Mac, Windows, Linux, Chrome OS, Android
[#enable-scroll-anchor-serialization](#)

Disable Audio For Desktop Share

With this flag on, desktop share picker window will not let the user choose whether to share audio. – Mac, Windows, Linux, Chrome OS, Android
[#disable-audio-support-for-desktop-share](#)



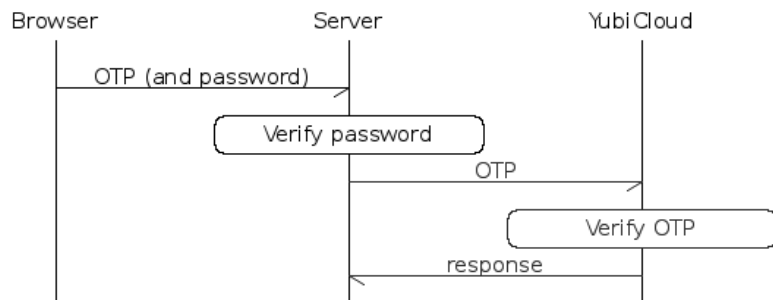


Índice

1. Safety & Security
2. Protocolo TLS 1.3
3. API Yubikey & YubiHSM
4. Maude-NPA protocol analyzer

Yubikey & YubiHSM

- Dispositivo USB de autenticación con soporte:
 - One-Time-Password (OTP), cifrado y autenticación de clave pública, FIDO U2F, Open Source.



Unique Device Id	Session Counter	Timestamp	Token Counter	Pseudo-random	CRC-16 value
8792ebfe26cc	0013	coa8 00	10	4495	e9ec



Yubikey

- Características complejas:
 - Contadores (tiempo discreto en forma de Lamport clocks)
 - Almacena claves y “nonces”
 - Propiedades basadas en eventos

Yubikey & YubiHSM

- Módulo hardware de seguridad (HSM) para proteger claves AES YubiKey
- Utiliza "Authenticated Encryption with Associated Data" (AEAD)
- Utiliza ó-exclusivo para cifrado criptográfico.



YubiHSM



Yubikey & YubiHSM

- Modelados y analizados usando Tamarin Prover en “YubiSecure? Formal Security Analysis Results for the Yubikey and YubiHSM” 8th International Workshop on Security and Trust Management (STM 2012)
 - (a) Ausencia de “replay attack” en YubiKey
 - (b) Correspondencia entre presionar el botón de YubiKey y un login con éxito.
 - (c) Contadores asociados a login en YubiKey son diferentes en el tiempo
 - (d) Si un intruso tiene acceso a YubiKey, donde se generan las claves AES, puede descifrar mensajes
 - (e) Si un intruso no tiene acceso a YubiKey, puede utilizar “nonces” de sesiones anteriores para obtener claves AES
- Modelados y analizados en Maude-NPA
- Probamos propiedades de seguridad (a,b,c)
- Encontramos ataques (d,e)

Attack Pattern	Depth								
	1	2	3	4	5	6	7	8	9
YubiKey (a)	4	4	9	21	88	160	0		
YubiKey (b)	4	7	16	14	2	2	5	0	
YubiKey (c)	4	4	6	18	55	80	0		
YubiKey Login	1	1	2	1	1	1	1	1	1(1)
YubiHSM (d)	1	2	3	4	7	13	24	40	76(1)
YubiHSM (e)	4	6	11	26(1)					



Índice

1. Safety & Security
2. Protocolo TLS 1.3
3. API Yubikey & YubiHSM
4. Maude-NPA protocol analyzer



Maude-NPA

- Herramienta de análisis para protocolos criptográficos (15 años de experiencia)

Santiago Escobar



Catherine Meadows



Jose Meseguer



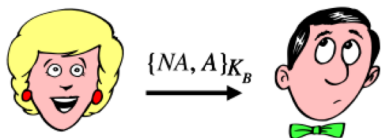
- Características principales: sesiones ilimitadas, teorías criptográficas avanzadas, Dolev-Yao activo, propiedades de secreto, autenticación e indistinguibilidad.
- Herramientas similares:
 - OFMC (DTU, Denmark)
 - Proverif (INRIA, France)
 - Tamarin (ETH Zurich, Switzerland)
 - CPSA (The MITRE Corporation, USA)

Protocolo Needham-Schroeder Public Key (NSPK)

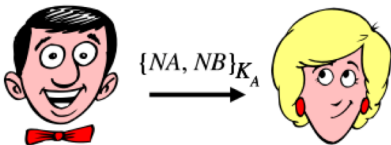
Maude-NPA

1. $A \rightarrow B : \{NA, A\}_{K_B}$
2. $B \rightarrow A : \{NA, NB\}_{K_A}$
3. $A \rightarrow B : \{NB\}_{K_B}$

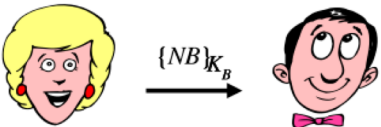
Objetivo: autenticación mutua. Traducción:



“Soy Alice y he elegido un nonce NA.”



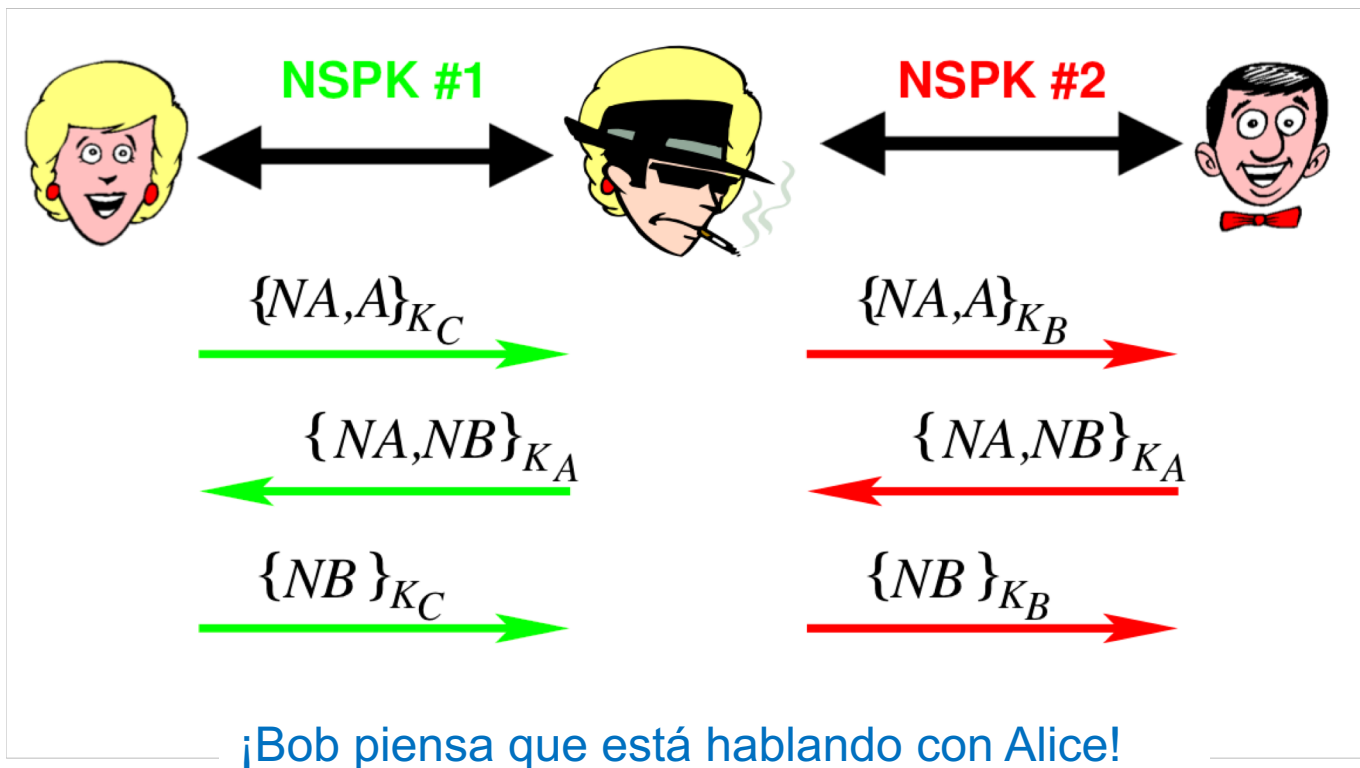
“Aquí tienes tu nonce NA. Ya que he podido leerlo, debo ser Bob. Aquí tienes mi nonce NB.”



“Me has enviado NB. Como solo Alice podía leerlo, y yo te lo he devuelto, tú debes de ser Alice.”

Man-in-the-middle attack

Maude-NPA



Maude-NPA

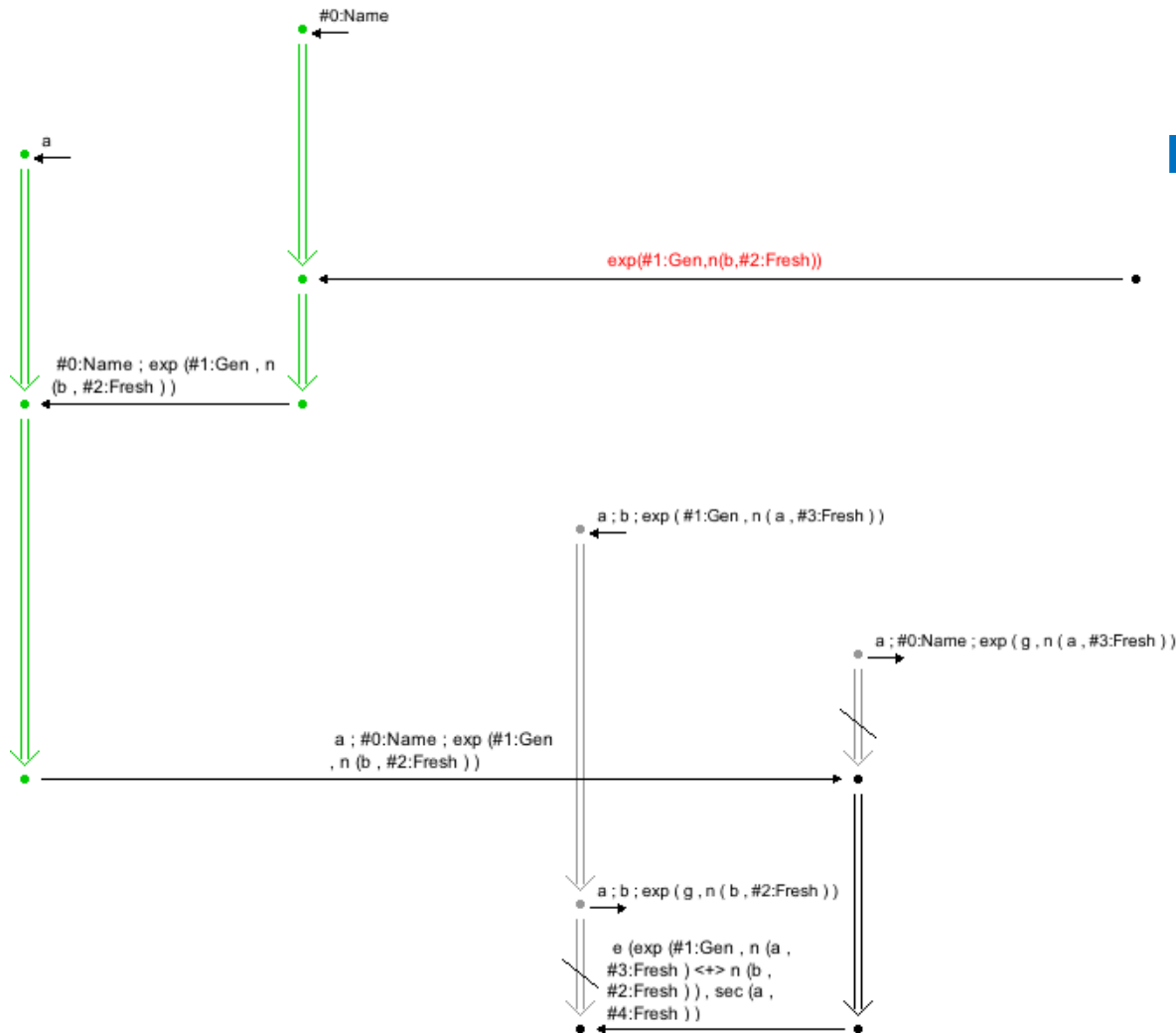
Modelo de ejecución: eventos de comunicación

$A \mapsto B : M_1$	$C \mapsto D : P_1$	$A \mapsto B : M_1$	$A \mapsto i_B : M_1$
$B \mapsto A : M_2$	$A \mapsto B : M_1$	$C \mapsto D : P_1$	$i_B \mapsto A : M_2$
	$B \mapsto A : M_2$	$i_B \mapsto A : M_2$	$A \mapsto i_B : M_3$
	$C \mapsto D : P_2$	$C \mapsto D : P_2$	

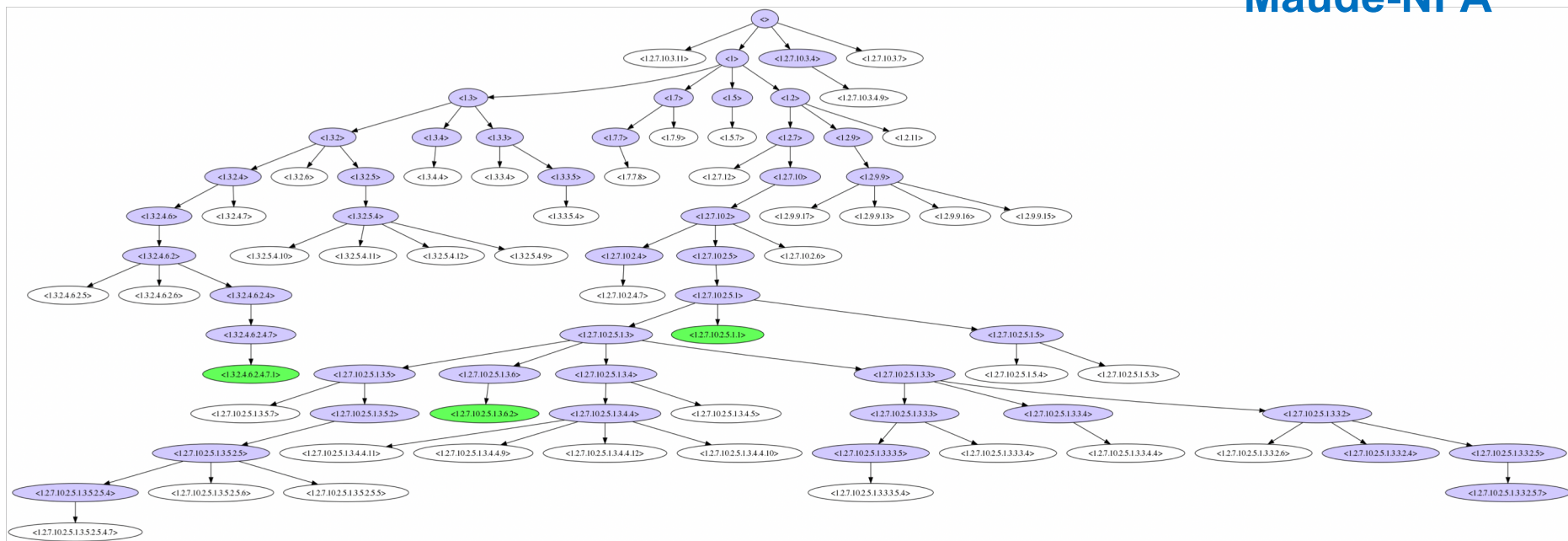
Una traza es una secuencia de eventos.

Análisis basado en entrelazado de sesiones del protocolo y acciones del intruso

Maude-NPA



Maude-NPA





Gracias!

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

➤ Síguenos en



ccn-cert
centro criptológico nacional

