Measuring Protocol Strength with Security Goals

HCSS

May 11, 2016

Paul D. Rowe, Joshua D. Guttman, Moses D. Liskov

The MITRE Corporation

{prowe, guttman, mliskov}@mitre.org

MITRE

Kerberos PKINIT Initialization Round

$$\begin{tikzcd}
C & & AS \\
\bullet \arrow[rr, "\llbracket ts_C, n_2 \rrbracket_{\mathsf{sk}(C)}, C, T, n_1"] \arrow[d, Rightarrow] & & \bullet \arrow[d, Rightarrow] \\
\bullet & & \bullet \arrow[ll, "\{\!| \llbracket k, n_2 \rrbracket_{\mathsf{sk}(A)} |\!\}_{\mathsf{pubk}(C)}, C, TGT, PKG"']
\end{tikzcd}$$

where:

$$\begin{aligned}
TGT &= \{\!| AK, C, ts_A |\!\}_{k_T} \\
PKG &= \{\!| AK, n_1, ts_A, T |\!\}_k
\end{aligned}$$

Attack on PKINIT

(Cervesato et al.)

$$\begin{tikzcd}[column sep=huge] C \arrow[r, "{[\![t_C, n_2]\!]_{\mathsf{sk}(C)}, C, T, n_1}"] \arrow[d, Rightarrow] & I \arrow[r, "{[\![t_C, n_2]\!]_{\boxed{\mathsf{sk}(I)}}, \boxed{I}, T, n_1}"] \arrow[d, Rightarrow] & AS \arrow[d, Rightarrow] \\ \bullet & \bullet \arrow[l, "{\{\!| [\![k, n_2]\!]_{\mathsf{sk}(A)} |\!\}_{\boxed{\mathsf{pubk}(C)}}, \boxed{C}, TGT, PKG}"'] & \bullet \arrow[l, "{\{\!| [\![k, n_2]\!]_{\mathsf{sk}(A)} |\!\}_{\mathsf{pubk}(I)}, I, TGT, PKG}"'] \end{tikzcd}$$

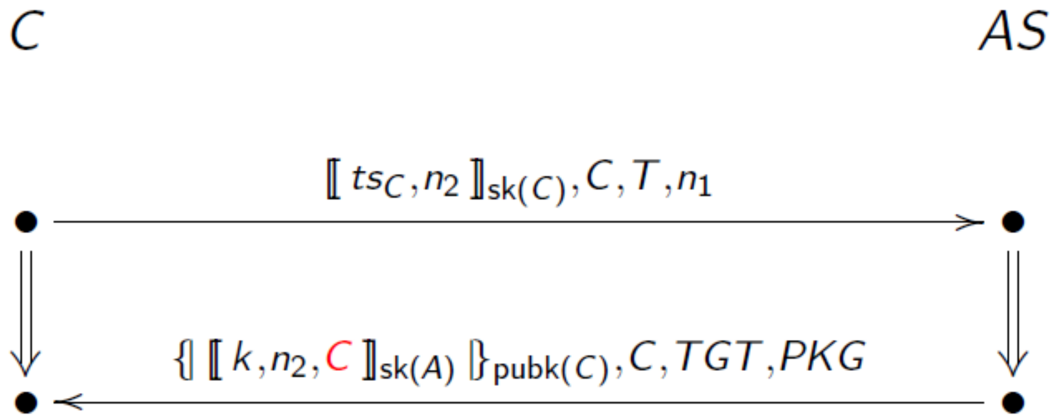
where:

$$\begin{aligned} TGT &= \{\!| AK, I, ts_A |\!\}_{k_T} \\ PKG &= \{\!| AK, n_1, ts_A, T |\!\}_k \end{aligned}$$

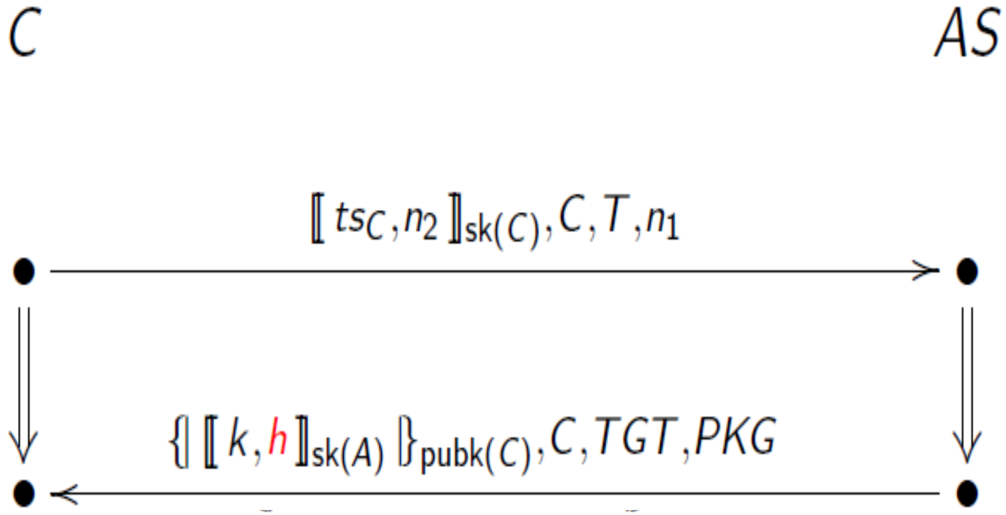
Intruder can eavesdrop on all subsequent communications.

How Do We Compare Proposed Fixes?

Fix #1



Fix #2



where: $h = hash([\![ts_C, n_2]\!]_{\mathsf{sk}(C)}, C, T, n_1)$

- **Which fix is "better"?**
  - Do they both mitigate the flaw?
  - Is one fix stronger than the other?
  - Against what measure?

MITRE

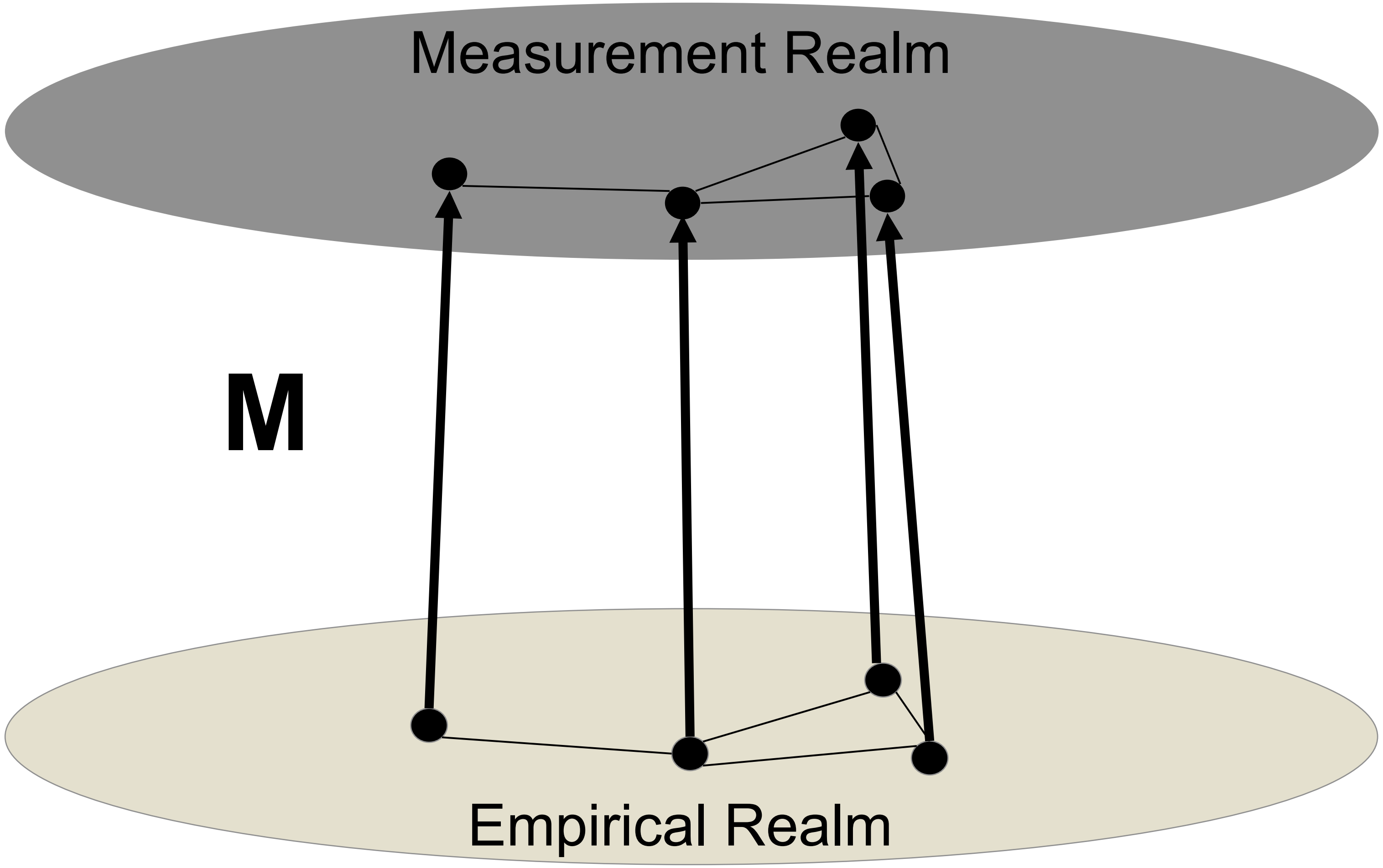
Main Contributions

- **Framework for systematically measuring relative security of (related) protocols**
  – Based on characterizing and comparing goals achieved by each
  – Always assuming all-or-nothing crypto and randomness (Dolev-Yao)

- **Subclass of goals relevant for enrich-by-need protocol analysis**
  – Syntactic subclass within a particular logical goal language
  – Distinguishing feature of tools like CPSA and Scyther

- **Potential interface to other tools and methods**
  – Common (tool-independent) language for expressing security goals

Idea of Measurement



MITRE

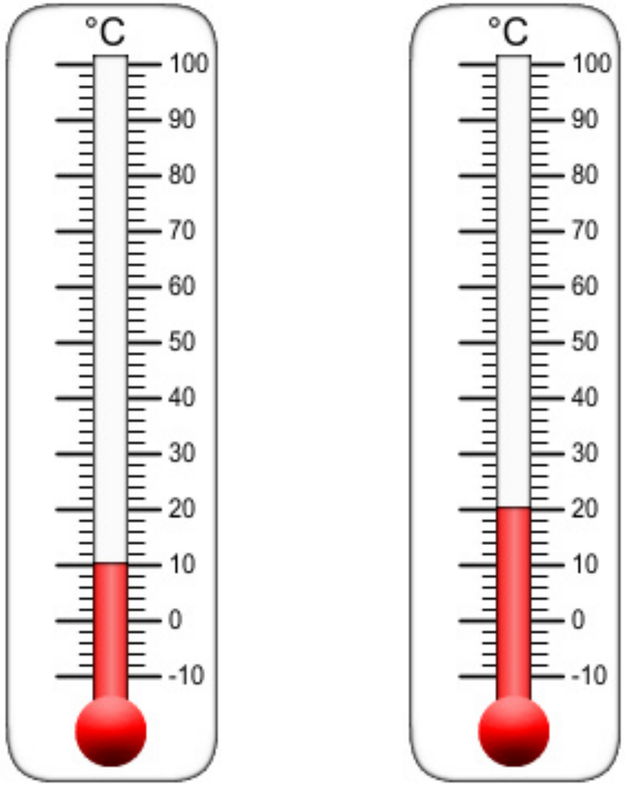
Measurement and Numerical Representation

Yesterday

10 C

Today

20 C



50 F

68 F

- **Is today twice as hot as yesterday?**
  - Temperature is only unique up to scale and 0
- **Choice of measurement representation should reflect relations of empirical realm**
  - Totally ordered representations are often inappropriate

Security is About Attacks and Goals

- **Π_1 is at least as secure as Π_2, if and only if any goal guaranteed by Π_2 is also guaranteed by Π_1 (with a given set of adversary capabilities).**

- **We write $\Pi_2 \ \underline{\blacktriangleleft}\ \Pi_1$ for the empirical ordering**

- **Protocols must be sufficiently similar to make sense of these concepts.**
  - E.g. Key secrecy should about “corresponding” keys
  - We do <u>not</u> strive to compare any arbitrary pair of protocols

Measurements: Sets of Logical Goal Formulas

- **Logical formulation of security goals is a natural representation choice**
  - **Measurement M yields sets of goals achieved by Π**
  - **Sets ordered by inclusion reflect empirical ordering**
- $M(S_1) \leq M(S_2) \quad iff \quad S_1 \,\underline{\blacktriangleleft}\, S_2$
- **We focus on authentication and secrecy goals**
  - Trace properties: Counterexamples are single executions

MITRE

Logical Structure of Security Goals

- **Authentication and secrecy goals have a particular logical structure**

$$\forall \overline{x} \,.\, (\Phi \implies \bigvee_{1 \le j \le i} \exists \overline{y}_j \,.\, \Psi_j)$$

- **Logical structure is independent of analysis tool or formalism**

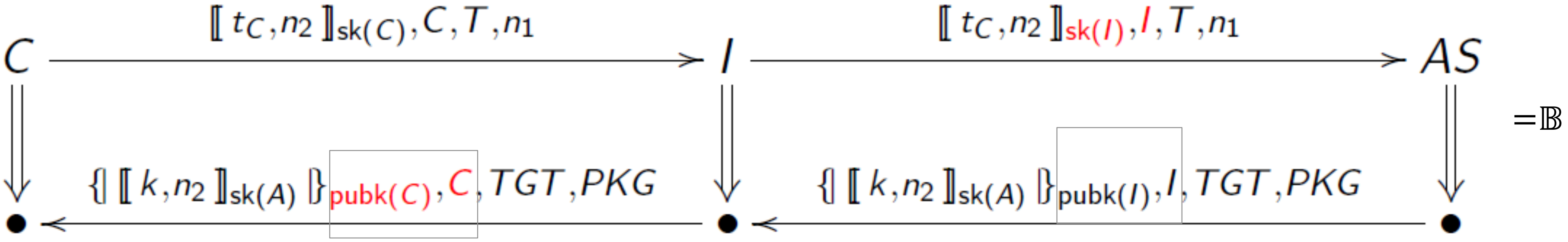
- **A single goal can be meaningful for many related protocols**
  - Common language separates goals from mechanisms to achieve them
  - “Related” is defined with respect to Guttman’s definition of protocol transformations

Example: PKINIT Security Goal

Security Goal Γ:

Whenever a client C processes a server's reply apparently from A containing server-generated credentials, then the server A previously produced those credentials for C.

Formula Satisfaction



$\mathbb{B} \vDash \phi$

$\mathbb{B} \vDash \psi$ /

$\mathbb{B} \vDash \Gamma$ /

$\mathtt{ASDone}(e') \wedge$

$\forall\, e, C, A, n_1, n_2\ .\ \phi \Rightarrow \exists\, e'\ .\ \psi$

$= \Psi$

$\mathtt{Nonce1}(e', n_1) \wedge$

$\ldots$

MITRE

Goal Satisfaction as a Security Measure

- **A protocol Π *achieves* a goal Γ iff every execution of Π satisfies Γ.**
- **Each set of goals $\mathcal{G}$ induces a lattice ordered by inclusion that serves as a scale to measure security.**
- **Let $\mathcal{G}$ be some set of goals, and let $M_{\mathcal{G}}(\Pi_i)=\{\Gamma\in\mathcal{G}\mid\Pi_i\ \textit{achieves}\ \Gamma\}$. Then**

$$\Pi_1 \blacktriangleleft_{\mathcal{G}} \Pi_2 \quad \textit{iff} \quad M_{\mathcal{G}}(\Pi_1)\subset M_{\mathcal{G}}(\Pi_2)$$

Measurement in the Two-Point Lattice

$\{\Gamma\}$ $\qquad$ $M(Fix_1) = M(Fix_2)$

$\{\,\}$ $\qquad$ $M(Orig)$

<u>Theorem 1:</u>

There exists a semi-decision procedure to determine if Π does not achieve Γ.

Measurement Granularity

- **Singleton sets yield a coarse scale for measurement**

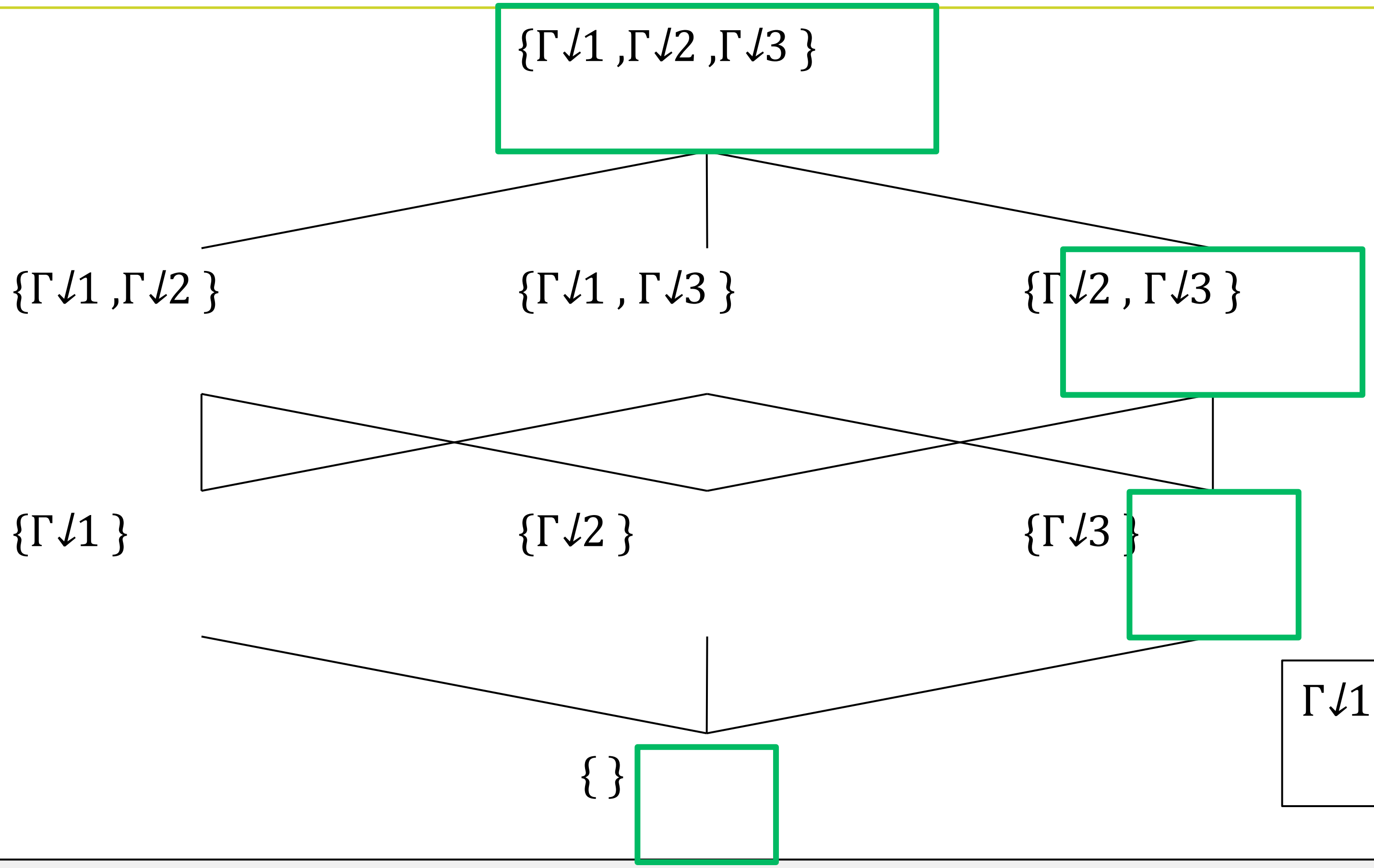
- **Larger sets of goals should provide more granularity**

<u>Theorem 2:</u>

Let $G' \subset G$ be sets of security goals.

If $\Pi_1 \blacktriangleright\!\blacktriangleleft_{G} \Pi_2$, then $\Pi_1 \blacktriangleright\!\blacktriangleleft_{G'} \Pi_2$

Finite Sets of Goals



Γ↓1 ⊨Γ↓2 ⊨Γ↓3

<u>Theorem 3:</u>

If Π achieves Γ and $\Gamma \models \Gamma'$, then Π also achieves Γ'.

Security Hierarchies in the Goal Language

- **Lowe's Hierarchy of Authentication:**
  - Weak Aliveness
  - Weak Agreement
  - Agreement ($d_1,\ldots,d_n$)
  - Injective Agreement

Weak aliveness.

$$\begin{pmatrix} \texttt{IDone}(n) \wedge \texttt{Peer}(n,r) \wedge \\ GoodKeys(n,\bar{k}) \end{pmatrix} \Rightarrow \begin{pmatrix} (\exists m\,.\,\texttt{RStart}(m) \wedge \texttt{Self}(m,r)) \vee \\ (\exists m\,.\,\texttt{IStart}(m) \wedge \texttt{Self}(m,r)) \end{pmatrix}$$

Weak agreement.

$$\Phi_1 \wedge \texttt{Self}(n,i) \quad \Rightarrow \quad (\Psi_1^1 \wedge \texttt{Peer}(m,i)) \vee (\Psi_1^2 \wedge \texttt{Peer}(m,i))$$

Weak agreement: Variant.

$$\Phi_1 \quad \Rightarrow \quad \begin{pmatrix} (\exists i\,.\,\Psi_1^1 \wedge \texttt{Self}(n,i) \wedge \texttt{Peer}(m,i)) \vee \\ (\exists i\,.\,\Psi_1^2 \wedge \texttt{Self}(n,i) \wedge \texttt{Peer}(m,i)) \end{pmatrix}$$

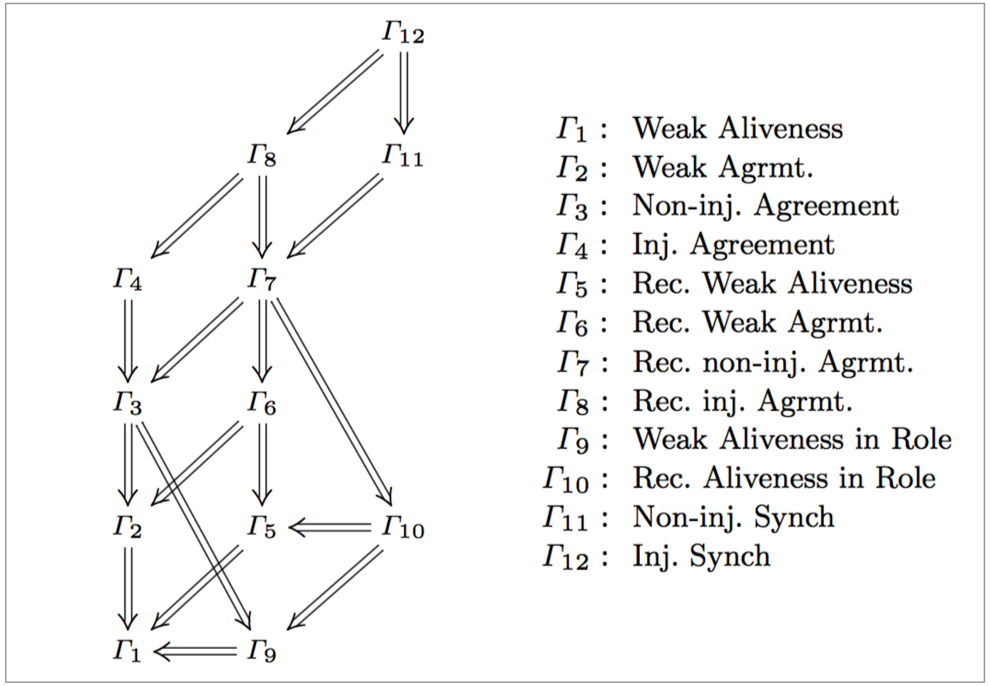
Non-injective agreement.

$$\Phi_2 \wedge \textstyle\bigwedge_{p \in V} \texttt{Param}_p(n, v_p) \quad \Rightarrow \quad \Psi_2^1 \wedge \textstyle\bigwedge_{p \in V} \texttt{Param}_p(m, v_p)$$

Injective session.

$$\Big(\texttt{IDone}(n_1) \wedge \textstyle\bigwedge_{p \in P(init)} \texttt{Param}_p(n_1, v_p) \wedge \quad \Big)$$

- **Cremers and Mauw's Additions:**
  - Weak Aliveness in Role
  - Synchronization
  - Injective synchronization



MITRE

An Infinite Set of Goals

- **Consider the infinite set of goals:** $\boldsymbol{H(\phi)=\{\Gamma \mid hyp(\Gamma)=\phi\}}$
- $\boldsymbol{M\uparrow H(\phi)\,(\Pi)}$ **always has a single maximum**
  - Relative to the implication order, up to bi-implication

<u>Theorem 4:</u>

Enrich-by-need analysis computes $\max[M\uparrow H(\phi)\ (\Pi)]$

<u>Corollary:</u>

$\boldsymbol{\Pi\downarrow 1} \blacktriangleleft \uparrow H(\phi)\, \boldsymbol{\Pi\downarrow 2}$ if and only if $\Pi\downarrow 2$ achieves $\max[M\uparrow H(\phi)\ (\Pi\downarrow 1\,)]$

Summary

- **Logical framework to formalize what it means to measure protocol security**
  - Framework has natural but clear scope of applicability
- **The framework unifies several approaches to defining security**
  - Repairs to a known flaw
  - Position in an authentication hierarchy
  - Richer, infinite sets: $H(\phi)$. Any others?
- **Our work suggests ways to compare/combine results of tools as well**
  - Could enable more rigorous independent verification
  - This would enhance the transparency of the standardization process

Measuring Protocol Strength with Security Goals

Thank You!

Questions?

Paul Rowe
The MITRE Corporation
prowe@mitre.org

MITRE