The Shapes of Protocols

Finding out what can happen

Joshua D. Guttman
Worcester Polytechnic Institute
The MITRE Corporation

March 2013
Bertinoro International Spring School

Thanks to the US National Science Foundation, under grant 1116557

guttman@wpi.edu

Let's start simple

Blanchet's Simple Example Protocol

$$
\begin{tikzcd}
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} & \{\!|\, s \,|\!\}_k \arrow[d] \\
\bullet \arrow[u] \arrow[r, Rightarrow] & \bullet
\end{tikzcd}
$$

$$
\begin{tikzcd}
\bullet \arrow[r, Rightarrow] & \bullet \arrow[d] \\
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} \arrow[u] & \{\!|\, s \,|\!\}_k
\end{tikzcd}
$$

What can happen, from initiator's point of view

Can K be disclosed?

$$\begin{tikzcd} \{\!| \{\!| k |\!\}_{\mathsf{sk}(A)} |\!\}_{\mathsf{pubk}(B)} & \bullet \arrow[l] \arrow[d, Rightarrow] & & \bullet & k \arrow[l] \\ & {} & & & \end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

What can happen, from initiator's point of view

Can K be disclosed?

$$\begin{tikzcd}
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} & \bullet \arrow[l] \arrow[d, Rightarrow] & & \bullet & k \arrow[l] \\
& {} & & &
\end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Adversary can't do it
since $\mathsf{pubk}(B)^{-1} \in \mathsf{non}$ and $k \in \mathsf{unique}$

What can happen, from initiator's point of view

Can K be disclosed?

$$\begin{tikzcd} \{\!|\ \{\!|\ k\ |\!\}_{\mathsf{sk}(A)}\ |\!\}_{\mathsf{pubk}(B)} & \bullet \arrow[l] \arrow[d, Rightarrow] & & \bullet & k \arrow[l] \\ & {} & & & \end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Are there any unintended services?

Unintended Services for k?

Blanchet's Simple Example Protocol

$$
\begin{tikzcd}
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} & \{\!|\, s \,|\!\}_{k} \arrow[d] \\
\bullet \arrow[u] \arrow[r, Rightarrow] & \bullet
\end{tikzcd}
$$

$$
\begin{tikzcd}
\bullet \arrow[r, Rightarrow] & \bullet \arrow[d] \\
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} \arrow[u] & \{\!|\, s \,|\!\}_{k}
\end{tikzcd}
$$

Unintended Services for k?

Blanchet's Simple Example Protocol

$$\begin{tikzcd}
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} & \{\!|\, s \,|\!\}_k \arrow[d] \\
\bullet \arrow[u] \arrow[r, Rightarrow] & \bullet
\end{tikzcd}$$

$$\begin{tikzcd}
\bullet \arrow[r, Rightarrow] & {\color{red}\bullet} \arrow[d] \\
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} \arrow[u] & \{\!|\, s \,|\!\}_k
\end{tikzcd}$$

Not a service for k because $k \not\sqsubseteq \{\!|\, s \,|\!\}_k$

What can happen, from initiator's point of view

Can K be disclosed?

$$\begin{tikzcd} \{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} & \bullet \arrow[l] \arrow[d, Rightarrow] & & \bullet & k \arrow[l] \\ & {} & & & \end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

So this is impossible
a secrecy goal

Diagram above is dead

The Nonce Test

Generalizing previous reasoning

Suppose $c \in$ unique originates at regular n_0
and in msg(n_1), $c \sqsubseteq$ msg(n_1) is found outside all the encryptions $S =$

$$\{\!|\, t_1 \,|\!\}_{K_1},\ \ldots,\ \{\!|\, t_j \,|\!\}_{K_j}$$

Then either:

1. One of the decryption keys $K_1^{-1}, \ldots, K_j^{-1}$ is disclosed before n_1, or
2. Some regular m_1 sends c outside S and
   - $m_1 \preceq n_1$
   - if $m_0 \Rightarrow^+ m_1$, c was found in msg(m_0) only within S if at all

The Nonce Test

Generalizing previous reasoning

Suppose $c \in$ unique originates at regular n_0
and in $\text{msg}(n_1)$, $c \sqsubseteq \text{msg}(n_1)$ is found outside all the encryptions $S =$

$$\{\!|\, t_1 \,|\!\}_{K_1},\ \ldots,\ \{\!|\, t_j \,|\!\}_{K_j}$$

Then either:

1. One of the decryption keys $K_1^{-1}, \ldots, K_j^{-1}$ is disclosed before n_1, or
2. Some regular m_1 sends c outside S and
   - $m_1 \preceq n_1$
   - if $m_0 \Rightarrow^+ m_1$, c was found in $\text{msg}(m_0)$ only within S if at all

We say that c escapes from S at m_1

Found outside

c is found outside S in t means:

Regarding t as an abstract syntax tree

there is a path p through the tree where

- $\mathrm{last}(p) = c$
- p never traverses key subterm of encryption $\{\!|\, t_1 \,|\!\}_K$
- p never traverses any $e \in S$

Found outside

c is found outside S in t means:

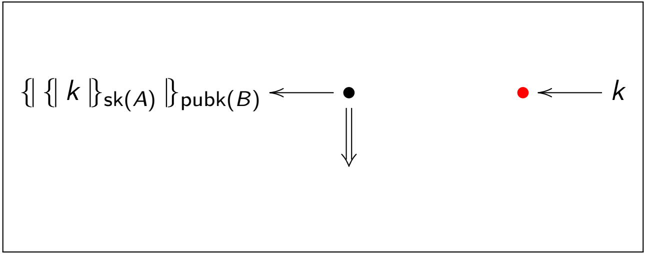
Regarding t as an abstract syntax tree

there is a path p through the tree where

- $\mathrm{last}(p) = c$
- p never traverses key subterm of encryption $\{\!|\, t_1 \,|\!\}_K$
- p never traverses any $e \in S$

You can get to an ingredient occurrence of c
without crossing anything in S

An Example



k is found outside $\{\!|\ k\ |\!\}_{\mathsf{sk}(A)}$ in k
but only within it in $\{\!|\ \{\!|\ k\ |\!\}_{\mathsf{sk}(A)}\ |\!\}_{\mathsf{pubk}(B)}$

Found only within

c is found only within S in t means:

Regarding t as an abstract syntax tree

for every path p through the tree where

- $\text{last}(p) = c$
- p never traverses key subterm of encryption $\{\!|\, t_1 \,|\!\}_K$

p traverses some $e \in S$

Found only within

c is found only within S in t means:

Regarding t as an abstract syntax tree

for every path p through the tree where

- $\text{last}(p) = c$
- p never traverses key subterm of encryption $\{\!|\, t_1 \,|\!\}_K$

p traverses some $e \in S$

You can't get to any ingredient occurrence of c
without crossing something in S

What can happen, from initiator's point of view

Another query $\mathbb{B}_1$ $\qquad$ t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$

$$\begin{tikzcd} \bullet \arrow[r] \arrow[d, Rightarrow] & t_0 \\ \bullet & \{\!|\, s \,|\!\}_k \arrow[l] \end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

What can happen, from initiator's point of view

Another query $\mathbb{B}_1$ $\qquad$ t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$

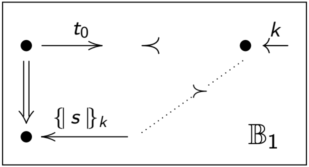
$$\begin{tikzcd} \bullet \arrow[r] \arrow[d, Rightarrow] & t_0 \\ \bullet & \{\!|\, s \,|\!\}_k \arrow[l] \end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Either k is disclosed,
or $\{\!|\, s \,|\!\}_k$ comes from a regular source

One of the two possible explanations $\mathbb{B}_1$

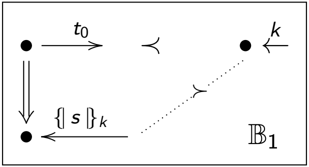
t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$



$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

One of the two possible explanations $\mathbb{B}_1$

t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$

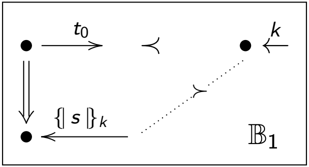


$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

By our previous result on $\bullet \xleftarrow{k}$, $\mathbb{B}_1$ is impossible

One of the two possible explanations $\mathbb{B}_1$

t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$



$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

By our previous result on $\bullet \xleftarrow{k}$, $\mathbb{B}_1$ is impossible

Principle: Dead if any substructure is dead

The other possible explanation $\mathbb{B}_2$

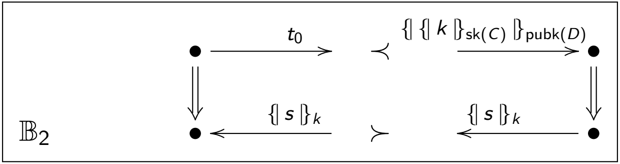
t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$

$$\mathbb{B}_2 \qquad \begin{tikzcd}
\bullet \arrow[r, "t_0"] \arrow[d, Rightarrow] & \prec \arrow[r, "\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(C)} \,|\!\}_{\mathsf{pubk}(D)}"] & \bullet \arrow[d, Rightarrow] \\
\bullet & \succ \arrow[l, "\{\!|\, s \,|\!\}_k"'] & \bullet \arrow[l, "\{\!|\, s \,|\!\}_k"']
\end{tikzcd}$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

The other possible explanation $\mathbb{B}_2$

t_0 is $\{\!|\ \{\!|\ k\ |\!\}_{\mathsf{sk}(A)}\ |\!\}_{\mathsf{pubk}(B)}$

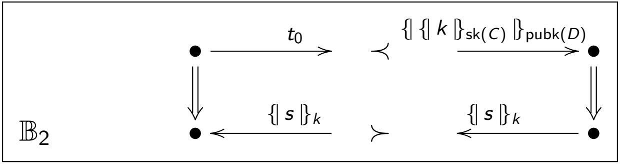


$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Do we know $C = A$ and $D = B$ in $\mathbb{B}_2$?

Nonce test applies to k in $\mathbb{B}_2$

t_0 is $\{\!|\ \{\!|\ k\ |\!\}_{\mathsf{sk}(A)}\ |\!\}_{\mathsf{pubk}(B)}$



Any service to build a new message t_1
with $k \sqsubseteq t_1$?

Unintended Services transforming k?

Blanchet's Simple Example Protocol

$$
\begin{tikzcd}
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} & \{\!|\, s \,|\!\}_{k} \arrow[d] \\
\bullet \arrow[u] \arrow[r, Rightarrow] & \bullet
\end{tikzcd}
$$

$$
\begin{tikzcd}
\bullet \arrow[r, Rightarrow] & \bullet \arrow[d] \\
\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)} \arrow[u] & \{\!|\, s \,|\!\}_{k}
\end{tikzcd}
$$

The other possible explanation $\mathbb{B}_2$

t_0 is $\{\!| \{\!| k |\!\}_{\mathsf{sk}(A)} |\!\}_{\mathsf{pubk}(B)}$

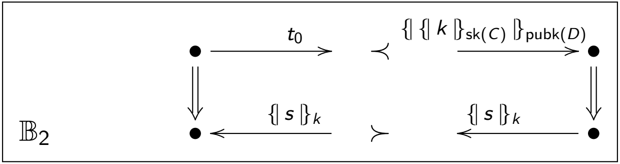
$$
\mathbb{B}_2 \qquad
\begin{tikzcd}
\bullet \arrow[r, "t_0"] \arrow[d, Rightarrow] & {} \arrow[r, phantom, "\prec"] & {} \arrow[r, "\{\!| \{\!| k |\!\}_{\mathsf{sk}(C)} |\!\}_{\mathsf{pubk}(D)}"] & \bullet \arrow[d, Rightarrow] \\
\bullet & {} \arrow[l, "\{\!| s |\!\}_k"'] \arrow[r, phantom, "\succ"] & {} & \bullet \arrow[l, "\{\!| s |\!\}_k"']
\end{tikzcd}
$$

$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Do we know $C = A$ and $D = B$ in $\mathbb{B}_2$?
Yes, since $C \neq A$ or $D \neq B$
would imply it's dead

The other possible explanation $\mathbb{B}_2$

t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$

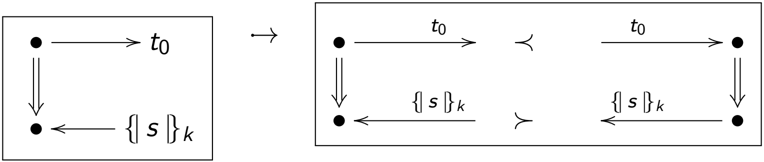


$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Do we know $C = A$ and $D = B$ in $\mathbb{B}_2$?
Yes, since $C \neq A$ or $D \neq B$
would imply it's dead

What did we prove?

t_0 is $\{\!|\, \{\!|\, k \,|\!\}_{\mathsf{sk}(A)} \,|\!\}_{\mathsf{pubk}(B)}$



$$\mathsf{pubk}(B)^{-1} \in \mathsf{non} \qquad k \in \mathsf{unique}$$

Any bundle containing at least $\mathbb{B}$
contains at least $\mathbb{B}_3$

A Tool to do this Reasoning: CPSA

Crypto Protocol Shape Analyzer

- Works with bundle fragments called skeletons starting from some $\mathbb{A}_0$
- While some skeleton $\mathbb{A}_i$ has unexplained parts, CPSA picks one
- Considers all enrichments $\mathbb{A}_j$ to explain it
- If none available, skeleton $\mathbb{A}_i$ is dead
- Branching stops when all parts explained
- Conclusion:

all bundles containing $\mathbb{A}_0$
contain one of its fully explained enrichments $\mathbb{A}_j$

The Encryption Test

Suppose that $\{\!|\, t \,|\!\}_K \sqsubseteq \text{msg}(n_1)$ where $n_1 \in \text{nodes}\mathbb{B}$. Then either:

1. Key K is disclosed before n_1 occurs,
   so that the adversary could construct $\{\!|\, t \,|\!\}_K$ from t; or
2. A regular $+$ node $m_1 \preceq n_1$ with

$$\{\!|\, t \,|\!\}_K \sqsubseteq \text{msg}(m_1)$$

   May choose m_1 least such