Firmalice

Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware

Yan Shoshitaishvili

Ruoyu "Fish" Wang

Christophe Hauser

Christopher Kruegel

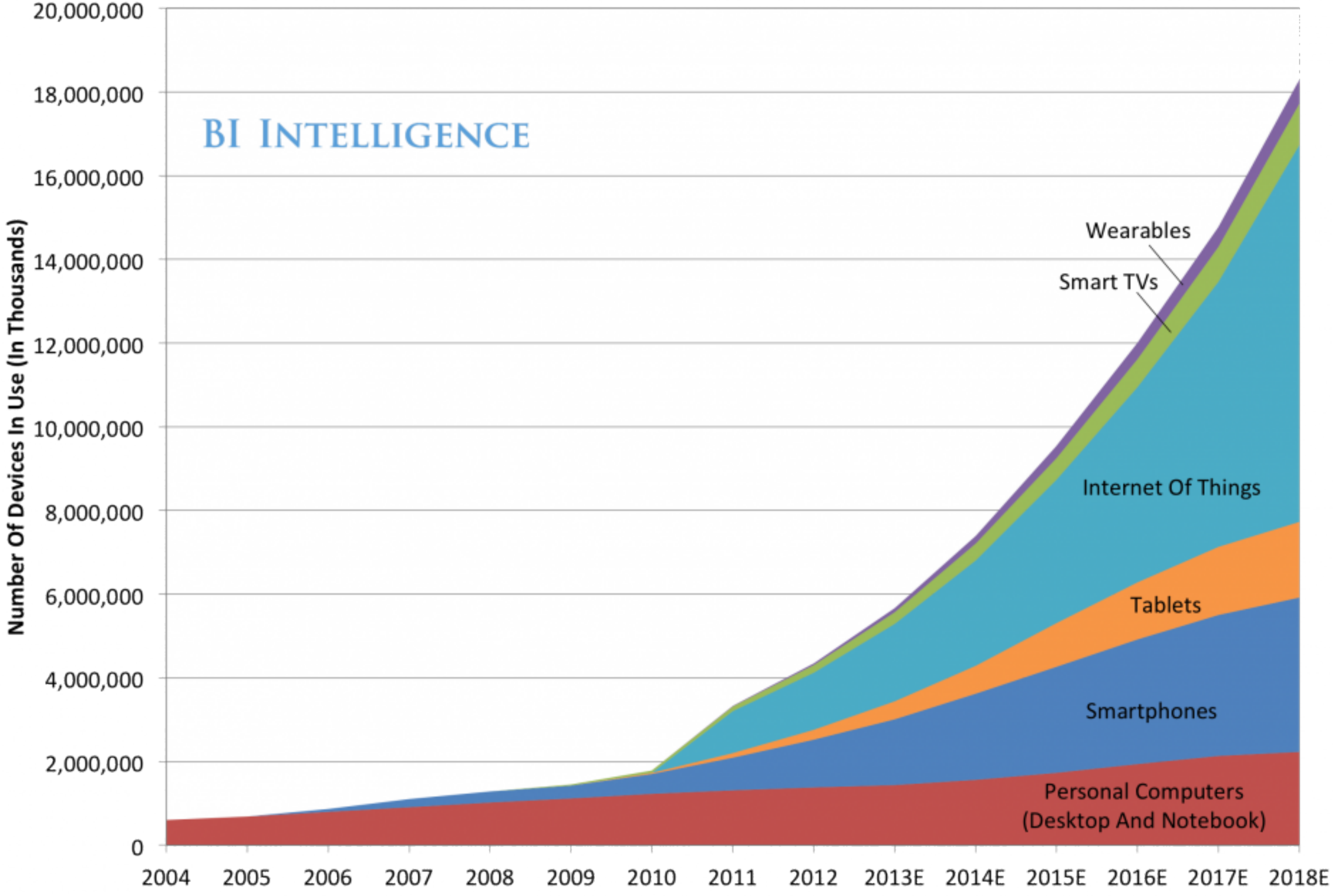
Giovanni Vigna

THE COMPUTER SECURITY GROUP AT UCSB

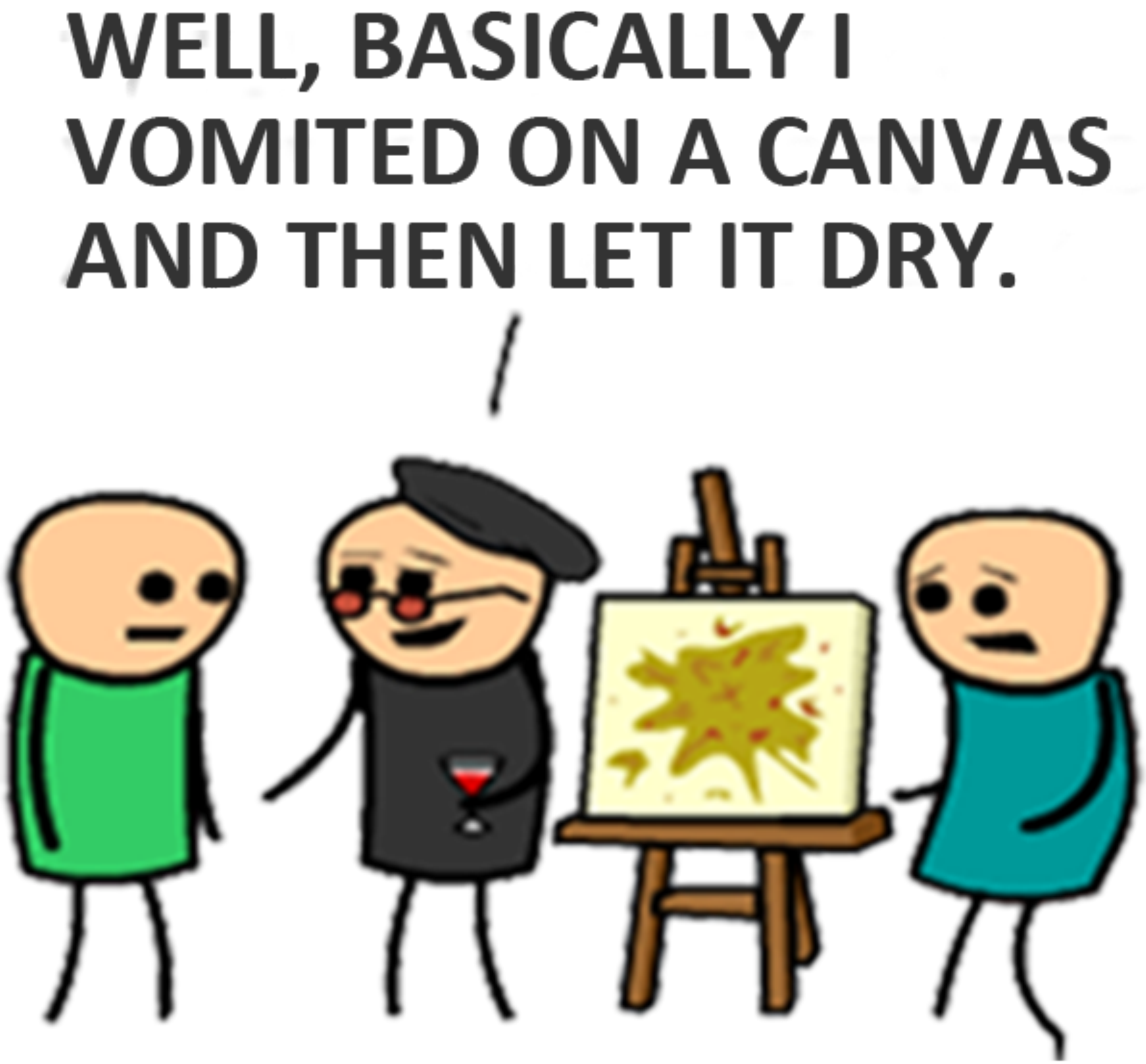
UC Santa Barbara

The Rise of Firmware

Global Internet Device Installed Base Forecast



Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BII estimates


WELL, BASICALLY I VOMITED ON A CANVAS AND THEN LET IT DRY.

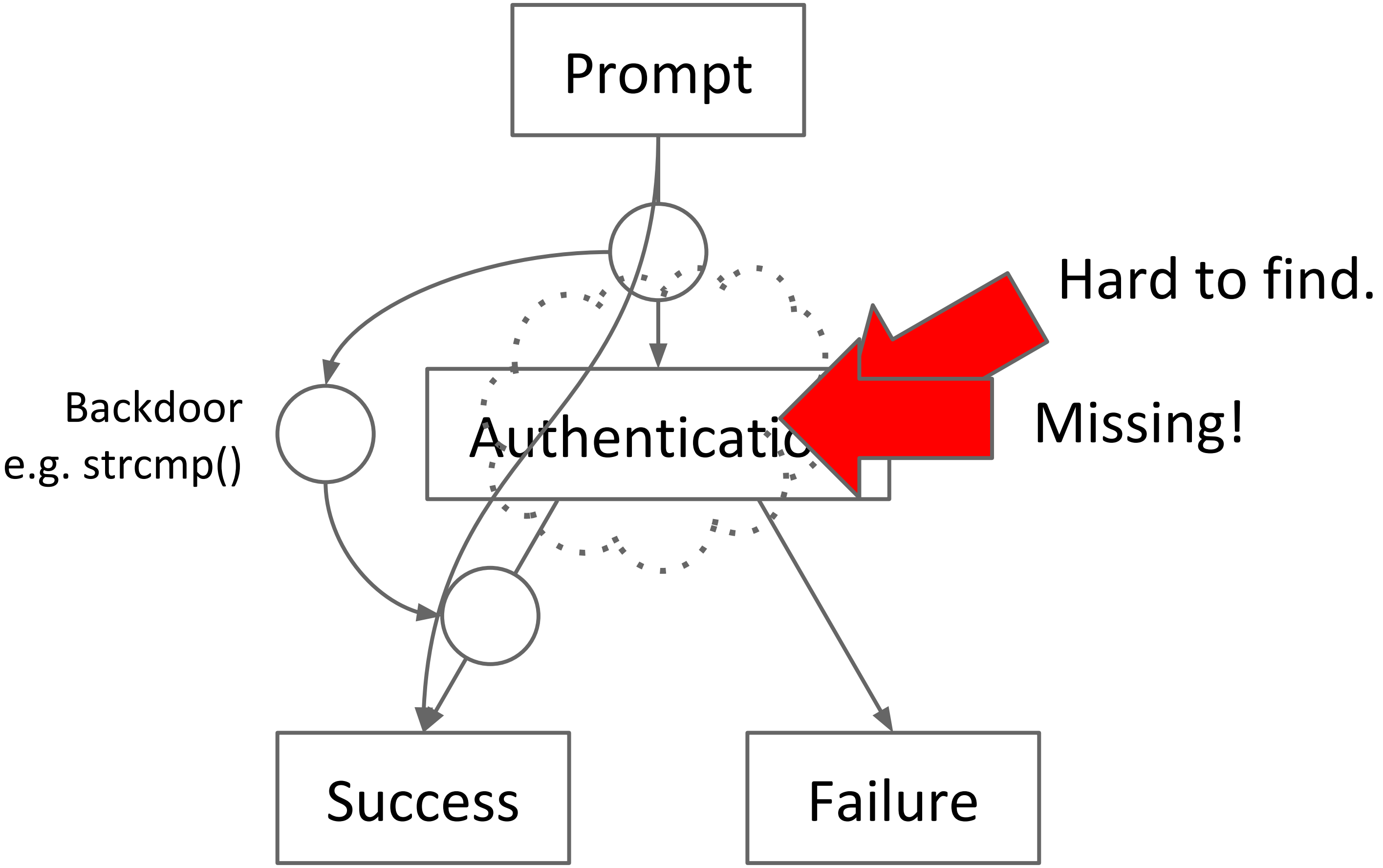
Emergence of Backdoors

Santamarta, Ruben. "HERE BE BACKDOORS: A Journey Into The Secrets Of Industrial Firmware." *Black Hat USA* (2012).

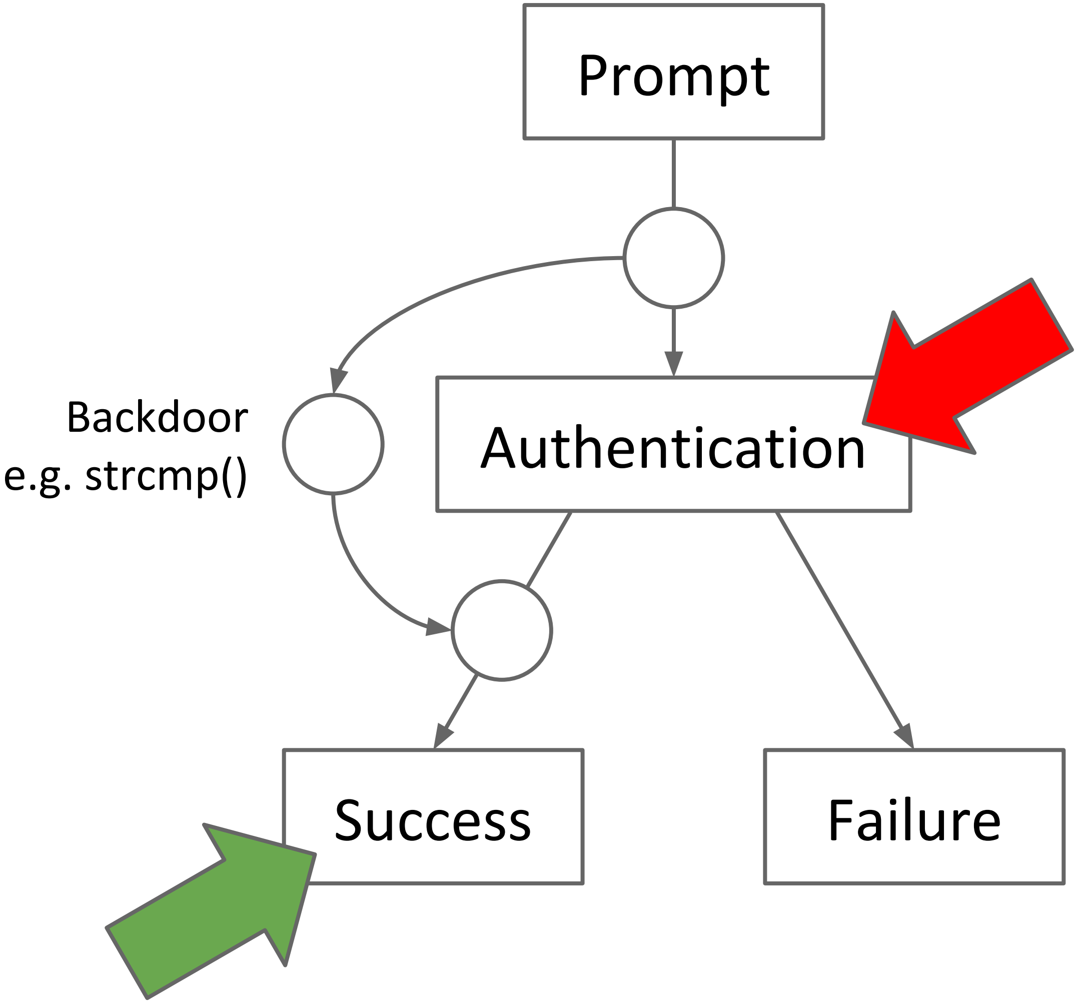
Heffner, Craig. "Reverse Engineering a D-Link Backdoor" /dev/ttys0 (2013).

Vanderbeken, Eloi. "TCP/32764 backdoor, or how linksys saved Christmas!" GitHub (2013).

Heffner, Craig. "Finding and Reversing Backdoors in Consumer Firmware." EELive! (2014).


Prompt
Backdoor
e.g. strcmp()
Authenticatio
Hard to find.
Missing!
Success
Failure

Our Solution: Input Determinism



Prompt

Backdoor
e.g. strcmp()

Authentication

Success

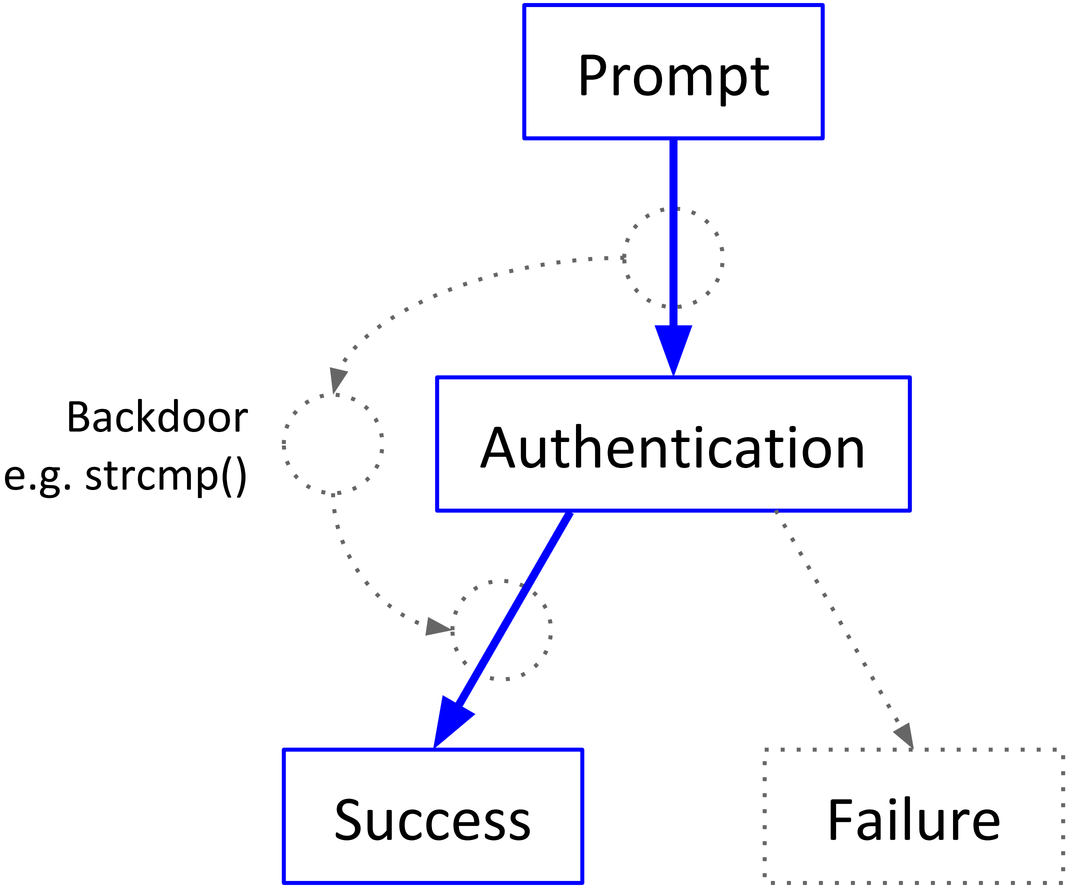
Failure

Hard to find.

Easier to find!

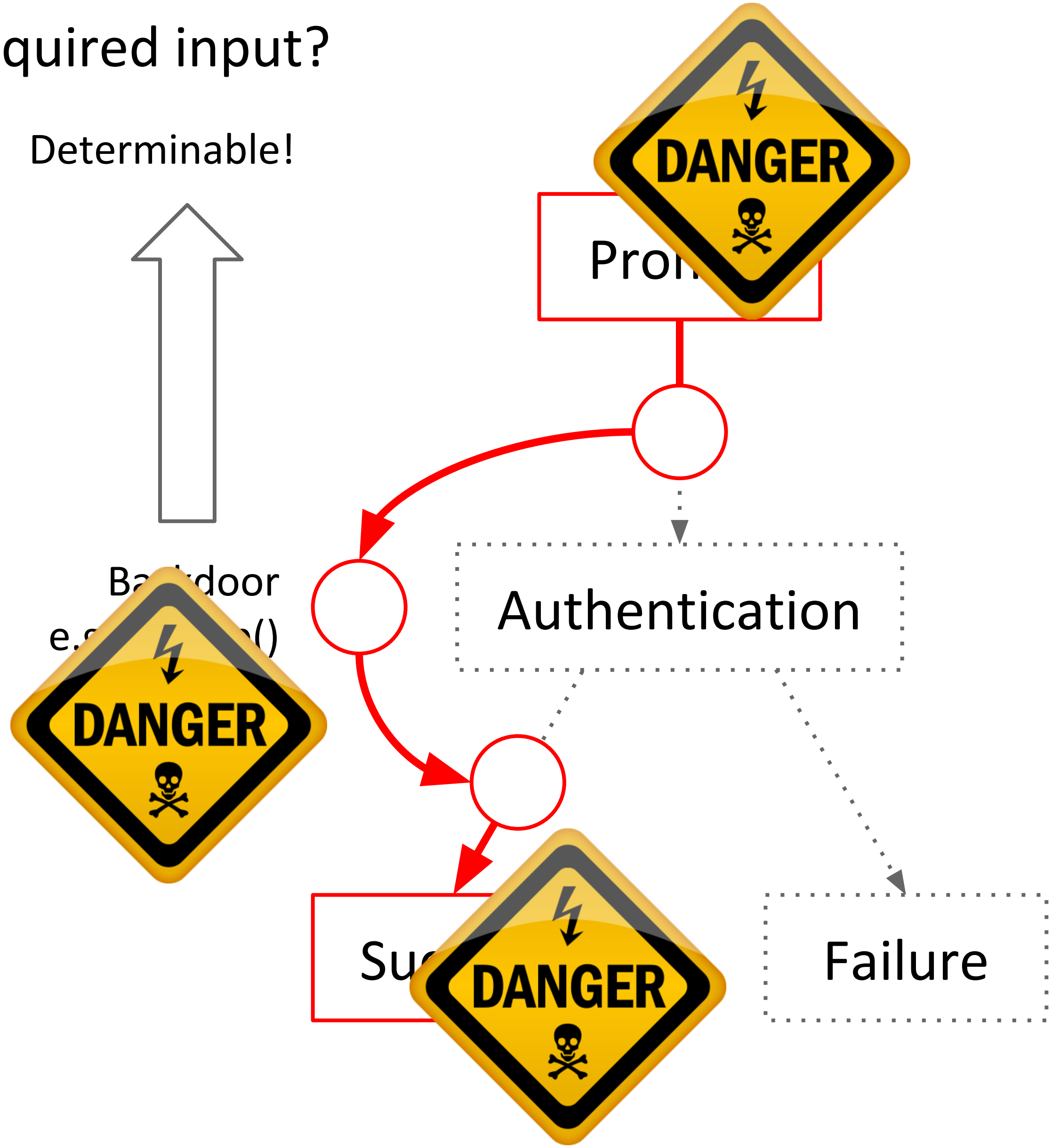
Required input?

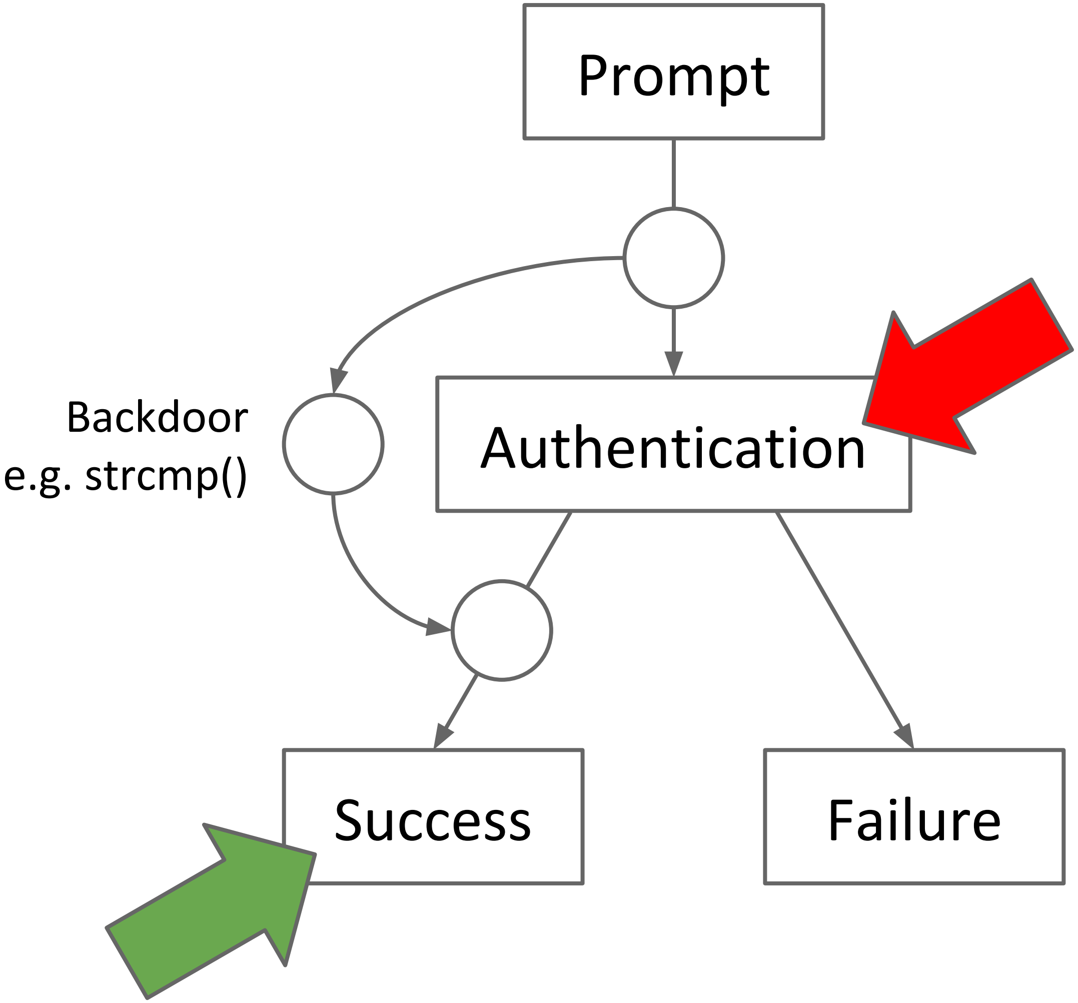
➔ Indeterminable



Required input?

→ Determinable!





Hard to find.

Easier to find, but how?

Security Policies

Se·cu·ri·ty Pol·i·cy

/səˈkyo͝orədē ˈpäləsē/ 🔊

noun

1. Identifies sensitive firmware functionality.
2. "By which point must a user be authenticated?"
3. Description of a *logical property* of the program.
4. Some heuristics for automatic identification.

Firmalice

Inputs:

→ Firmware Sample

→ Security Policy

Challenges:

→ Large binary programs

→ Unrelated user input

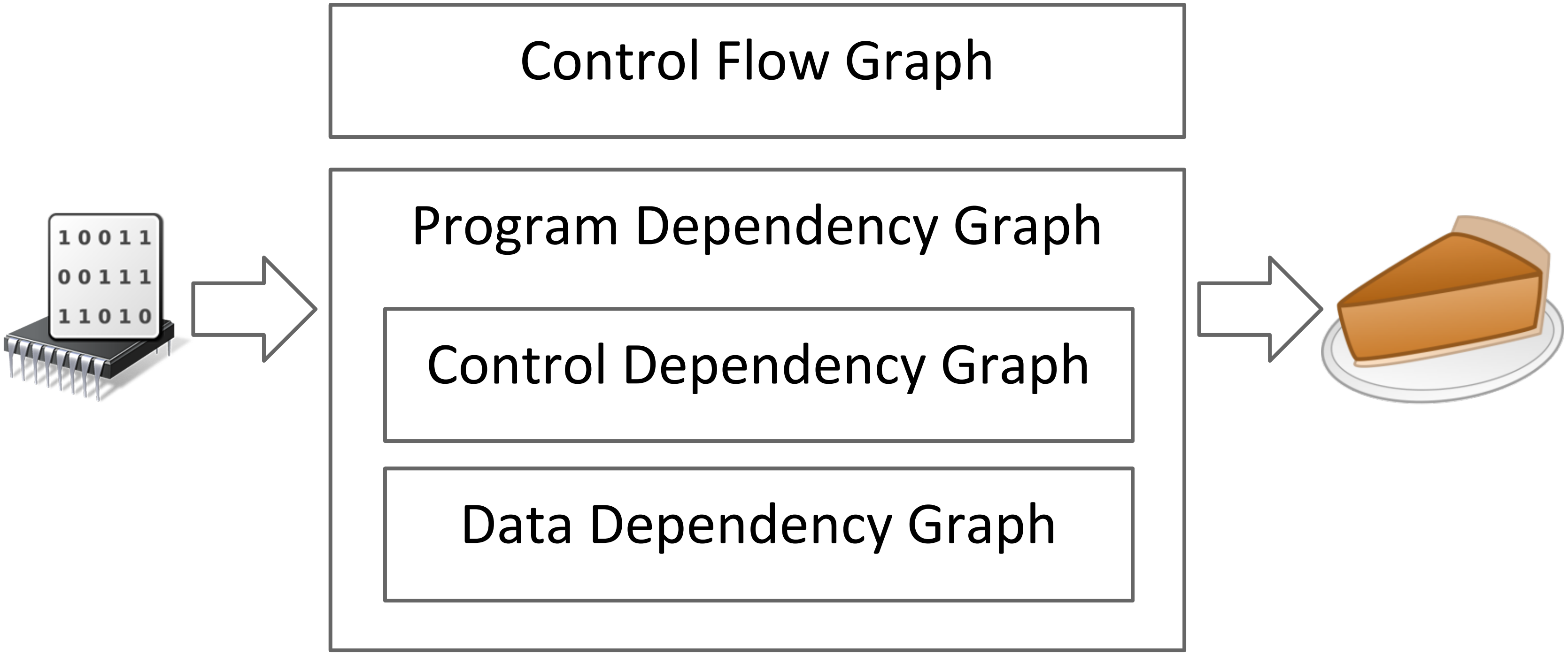
Analysis Steps:

→ Static Analysis (backwards program slicing)

→ Dynamic Symbolic Execution

→ Authentication Bypass Check

Static Analysis

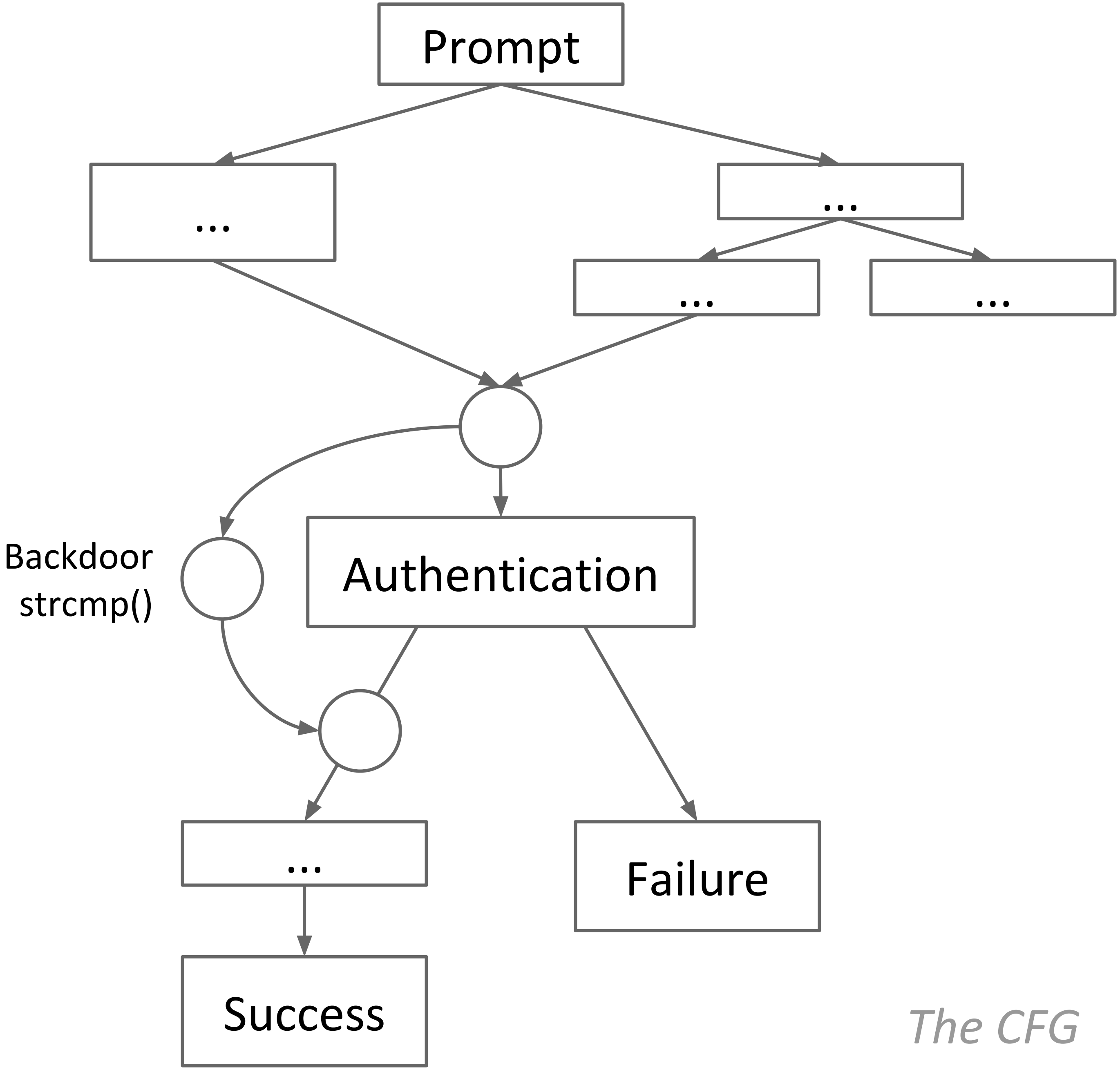


Control Flow Graph

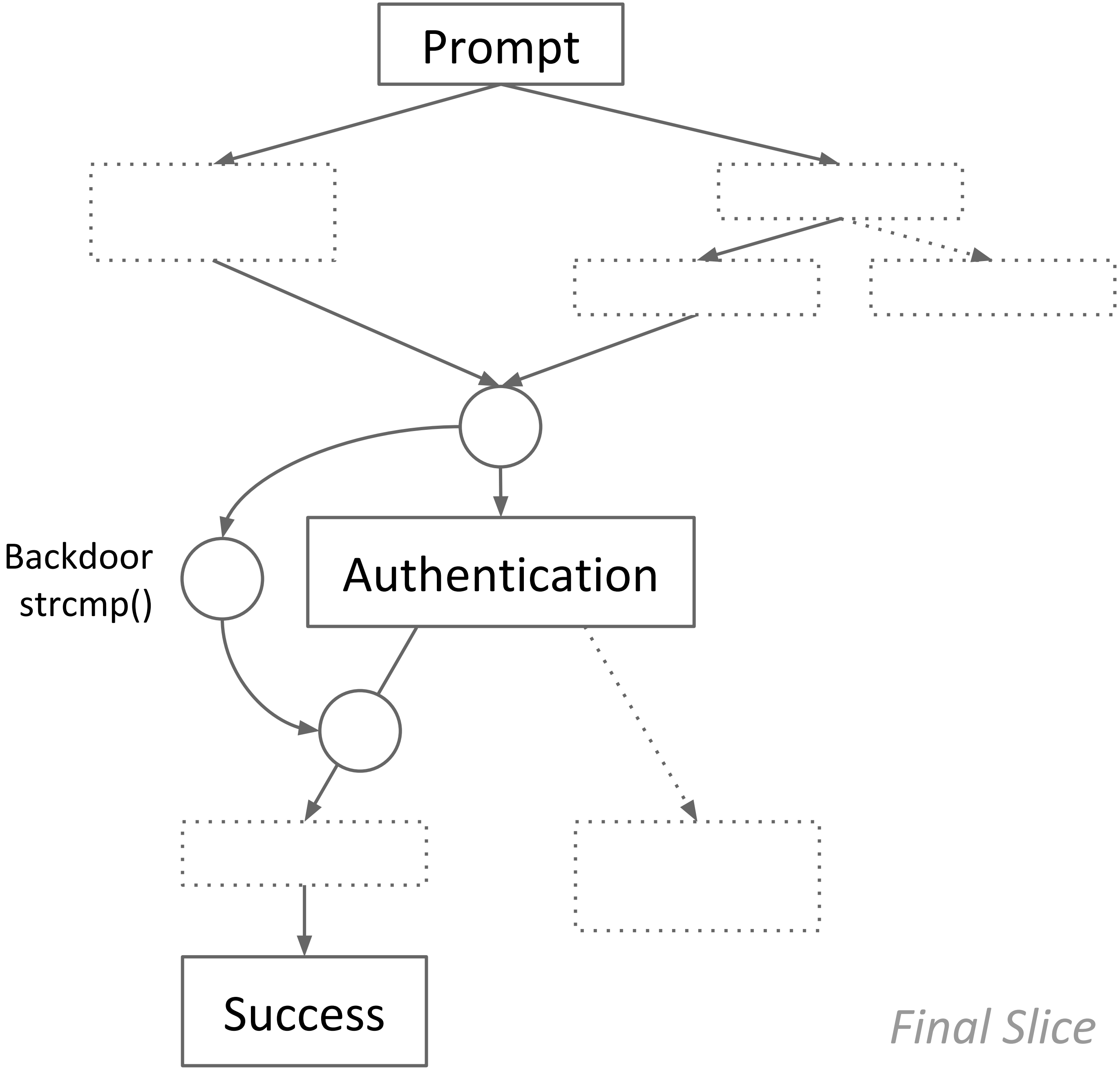
Program Dependency Graph

Control Dependency Graph

Data Dependency Graph

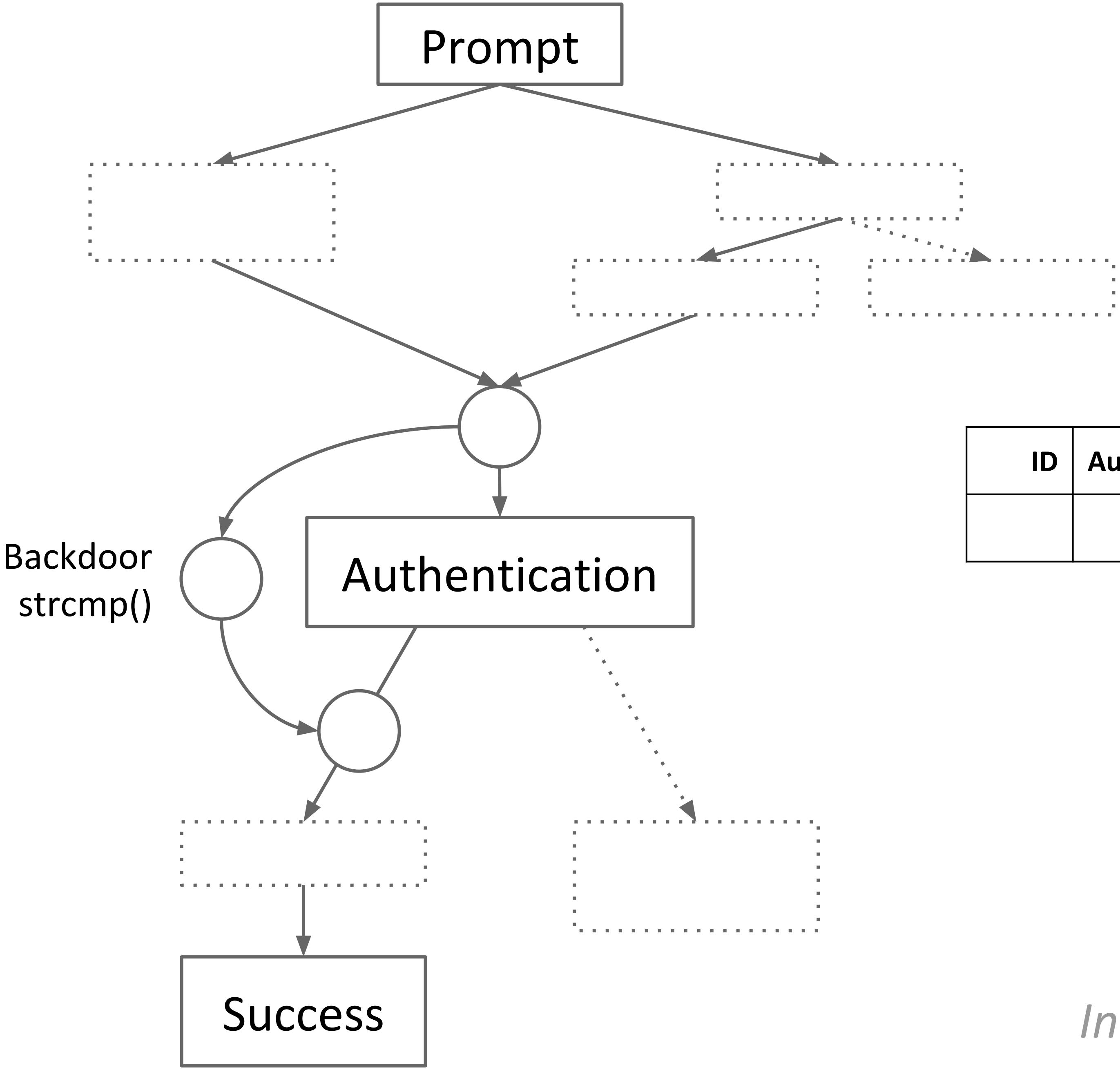


The CFG



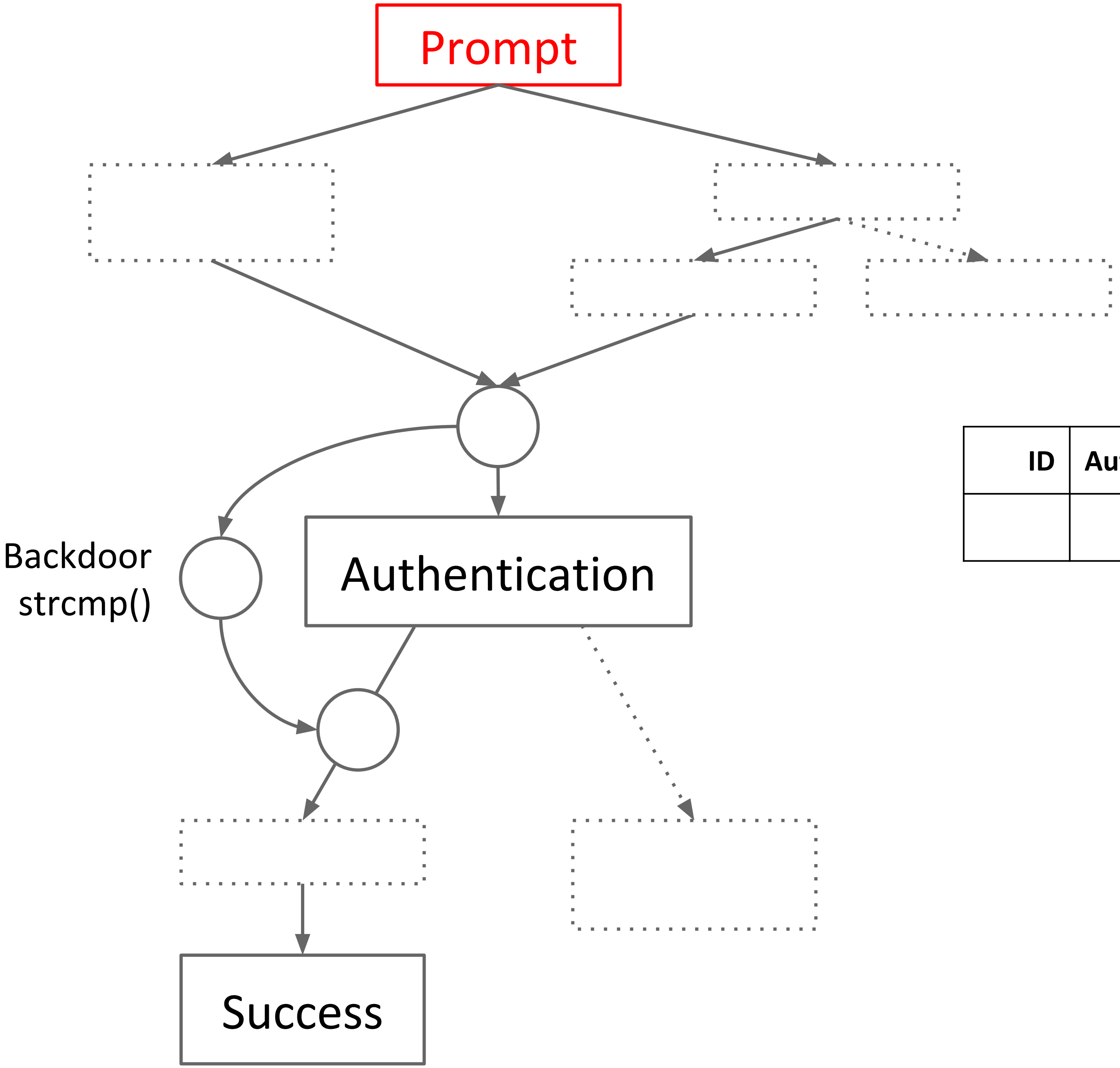
Final Slice

Dynamic Symbolic Execution



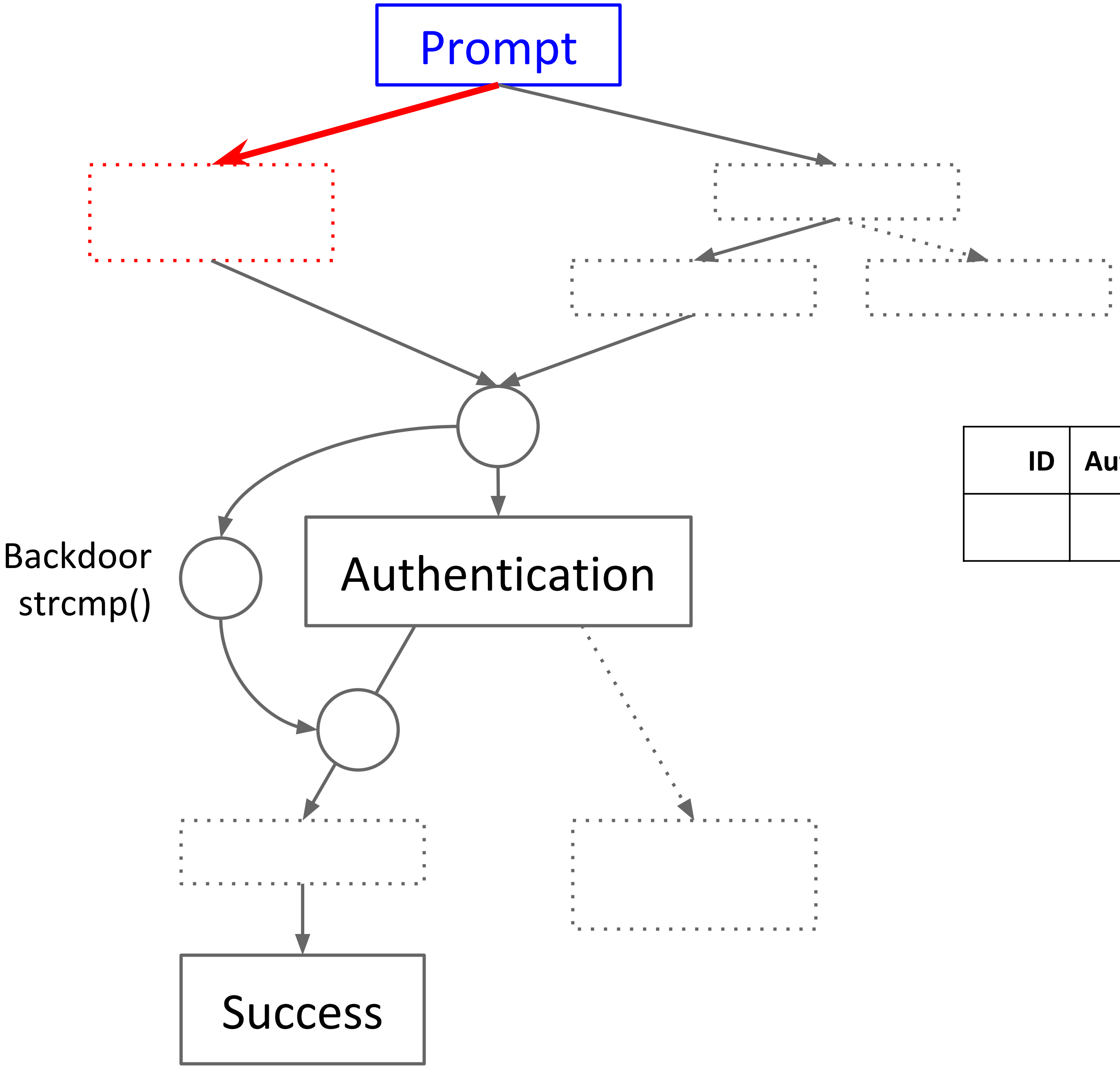
ID	Authenticated Paths

Initial Stage



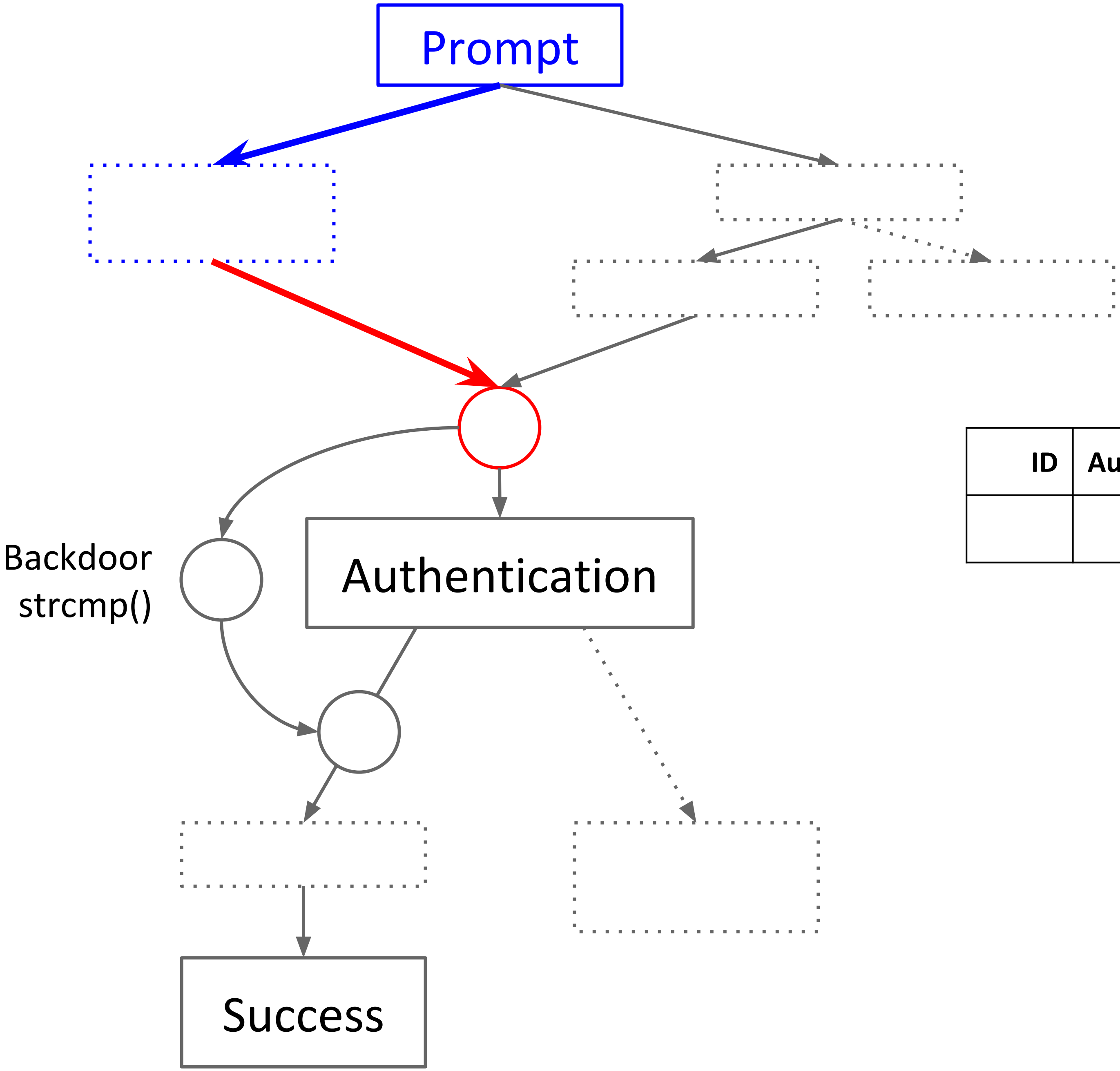
ID	Authenticated Paths

Step 1



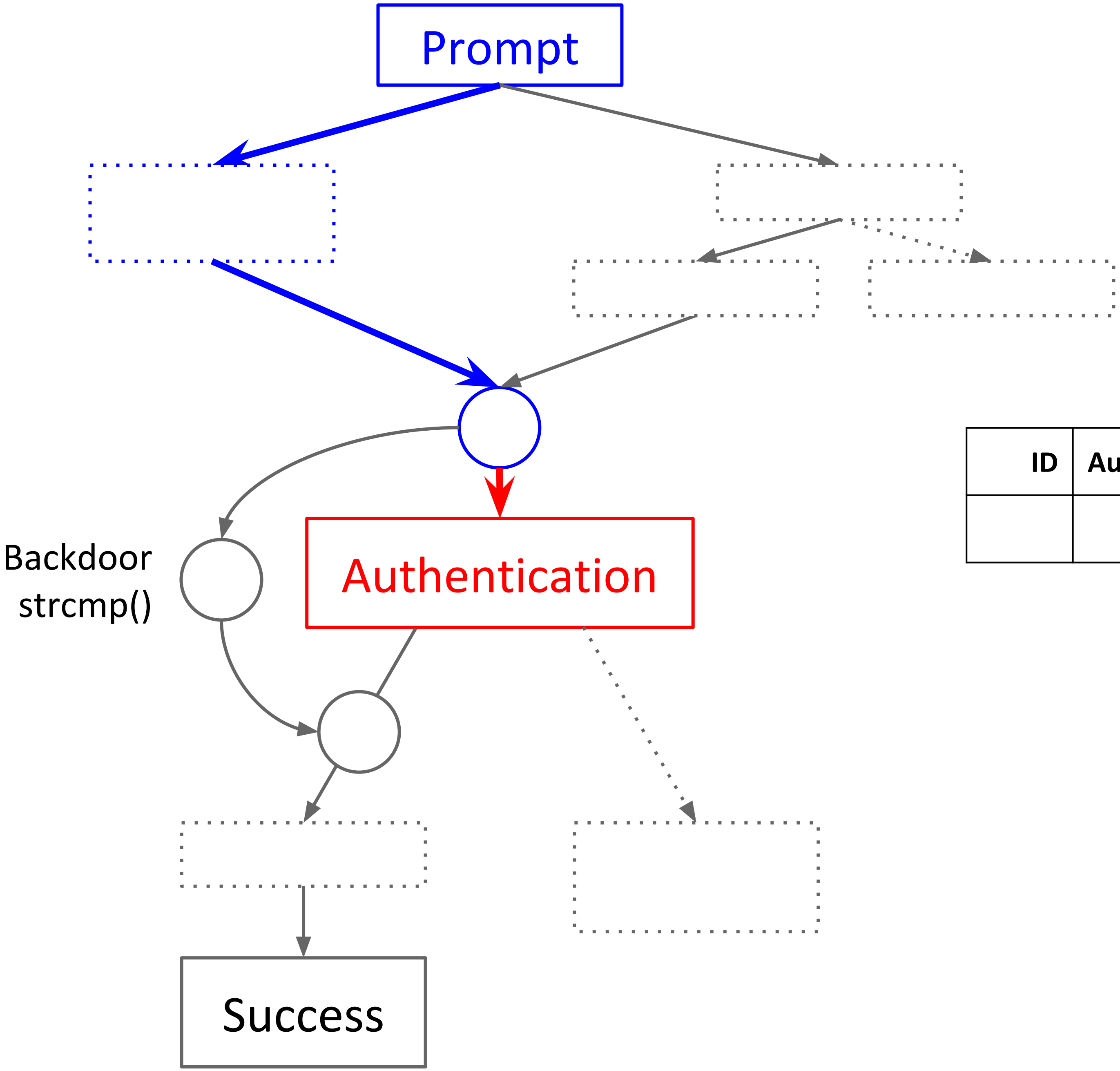
ID	Authenticated Paths

Step 2



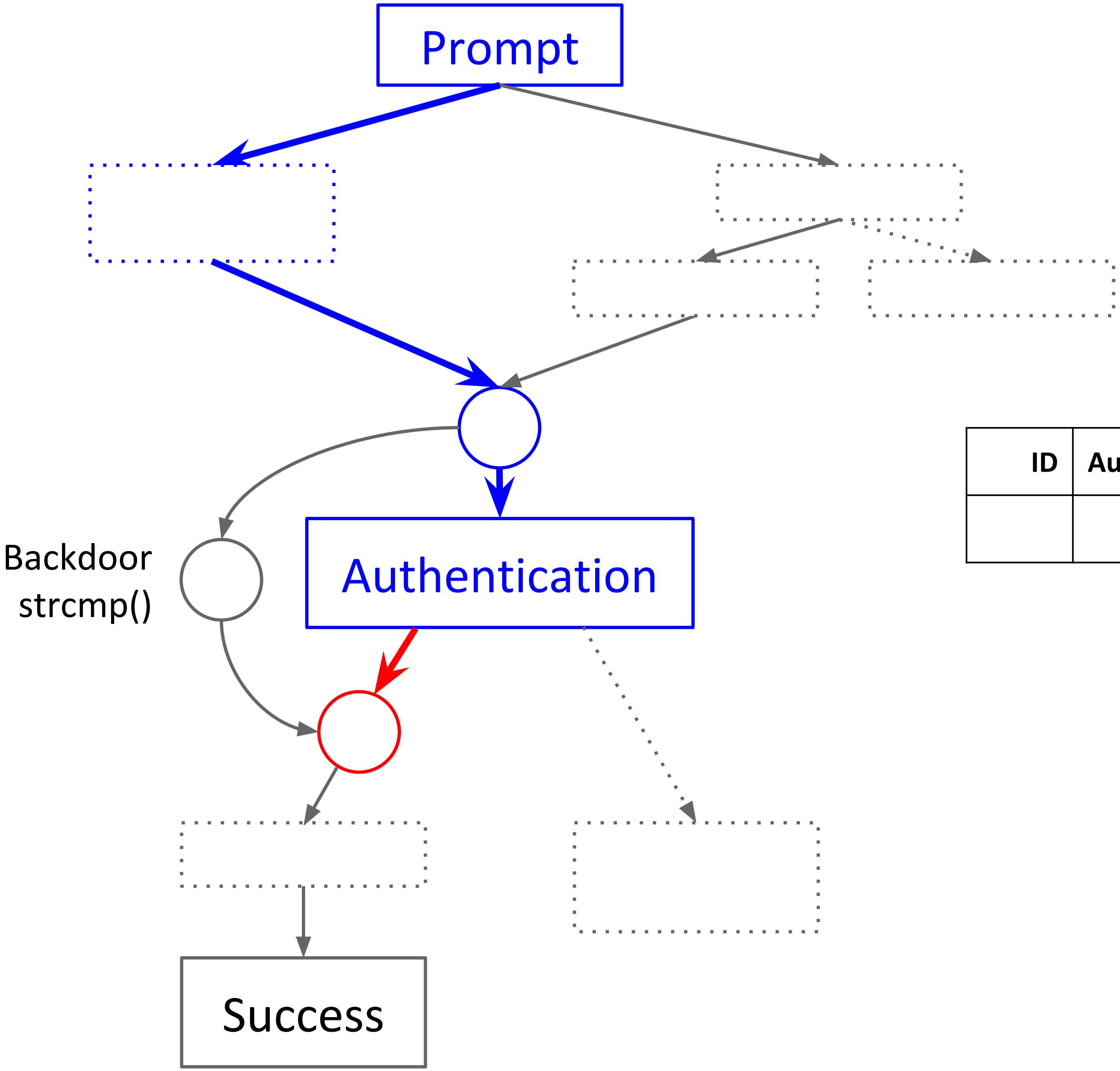
ID	Authenticated Paths

Step 3



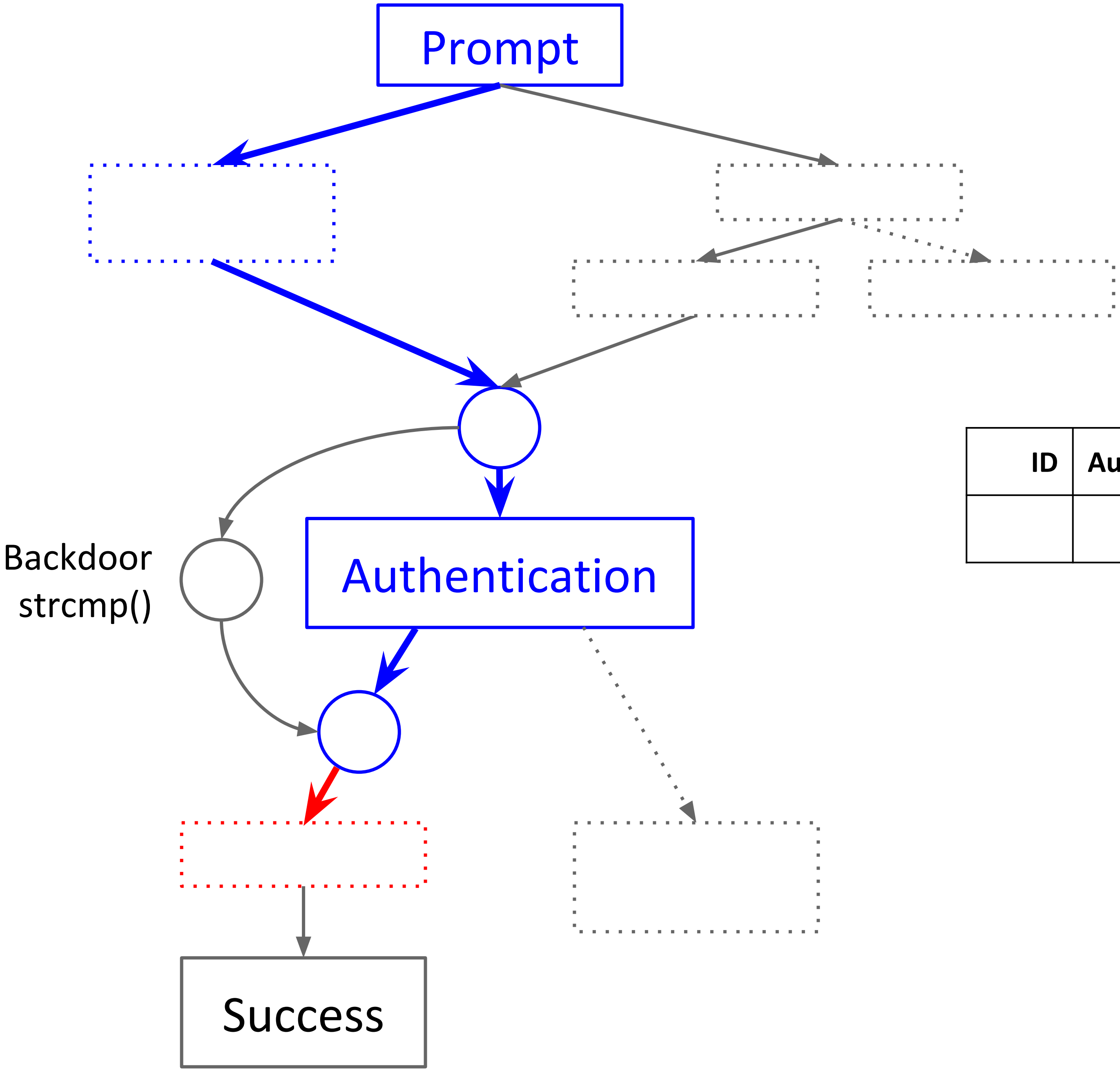
ID	Authenticated Paths

Step 4



ID	Authenticated Paths

Step 5



Prompt

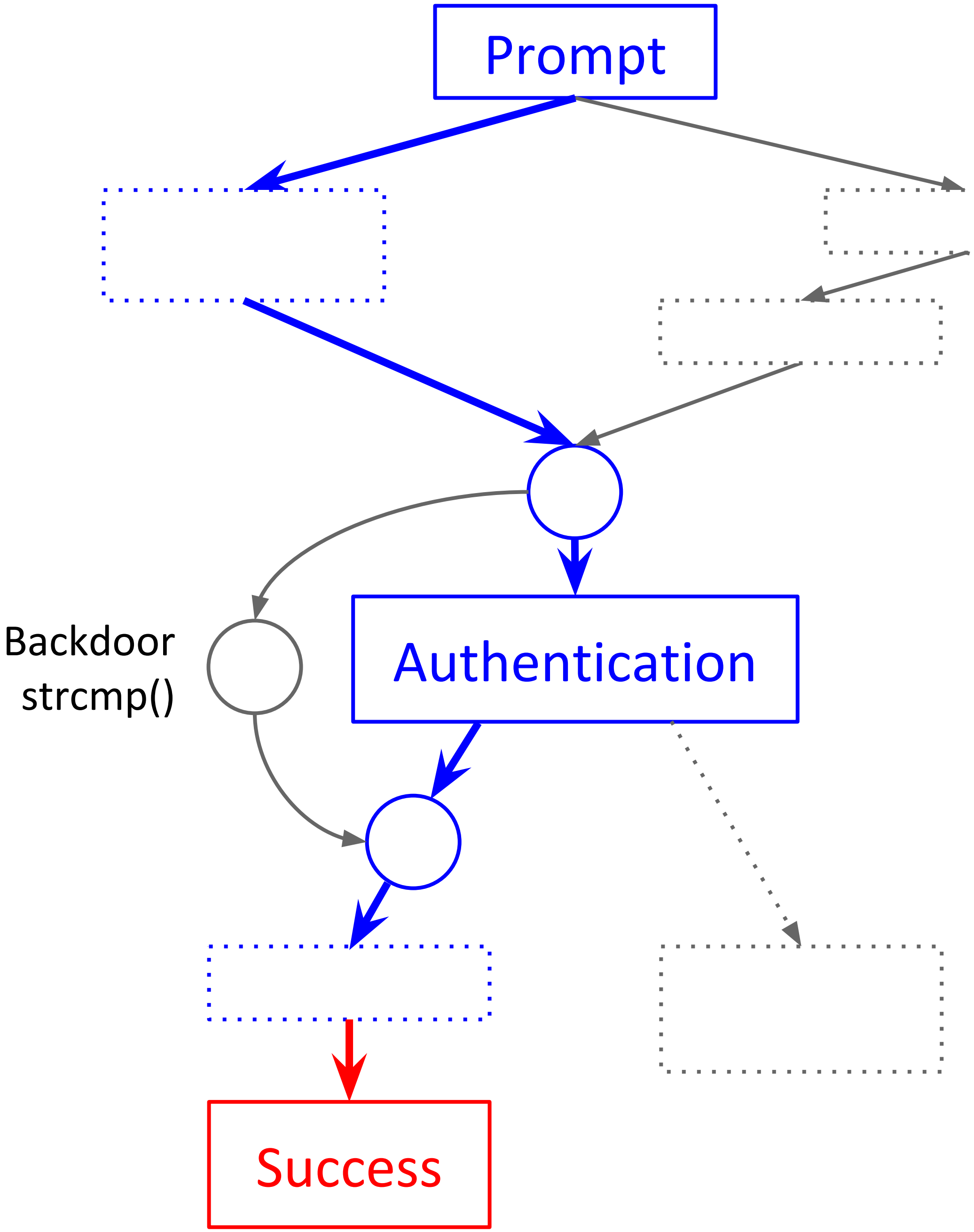
Backdoor strcmp()

Authentication

Success

ID	Authenticated Paths

Step 6



Prompt

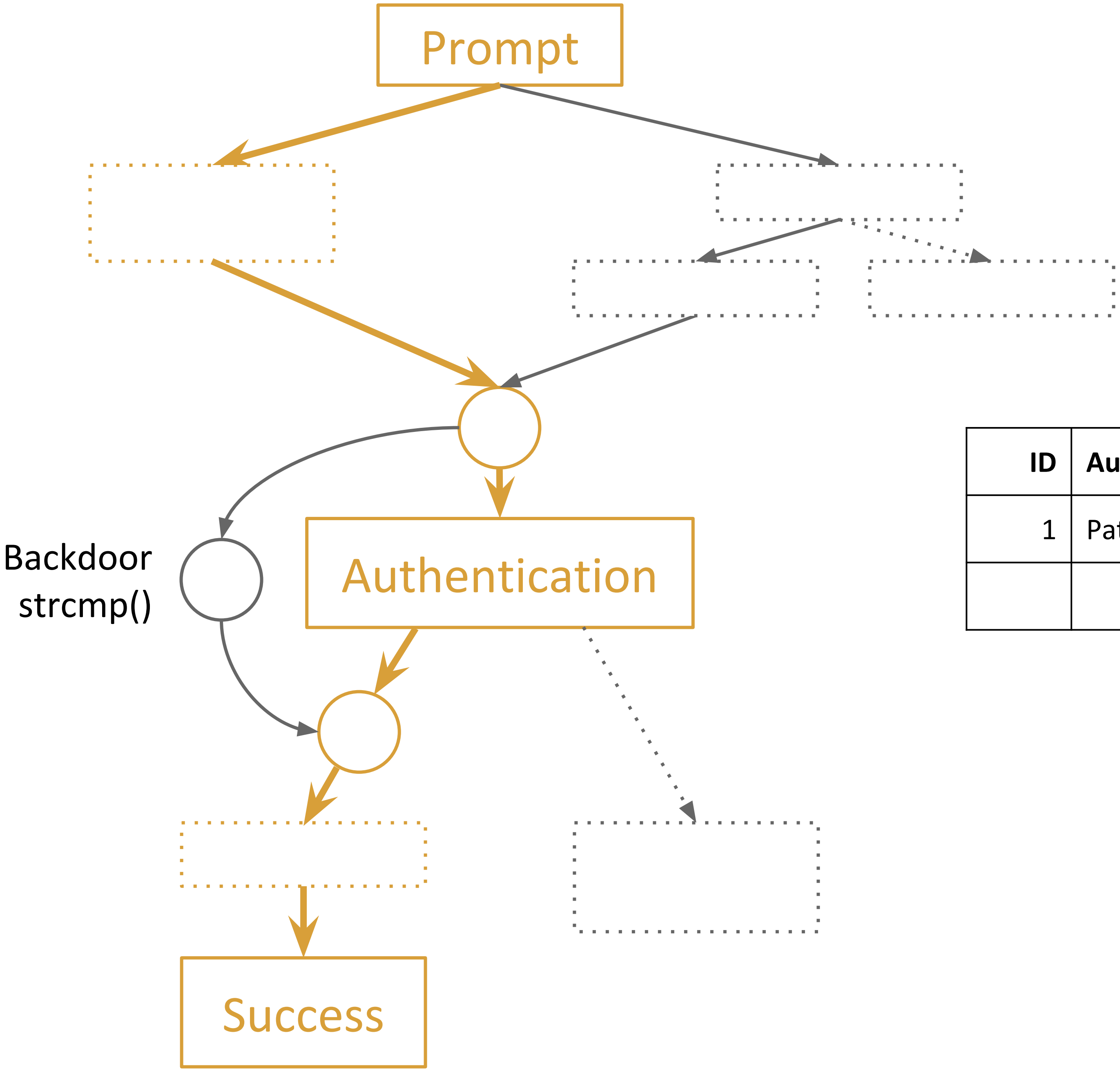
Backdoor
strcmp()

Authentication

Success

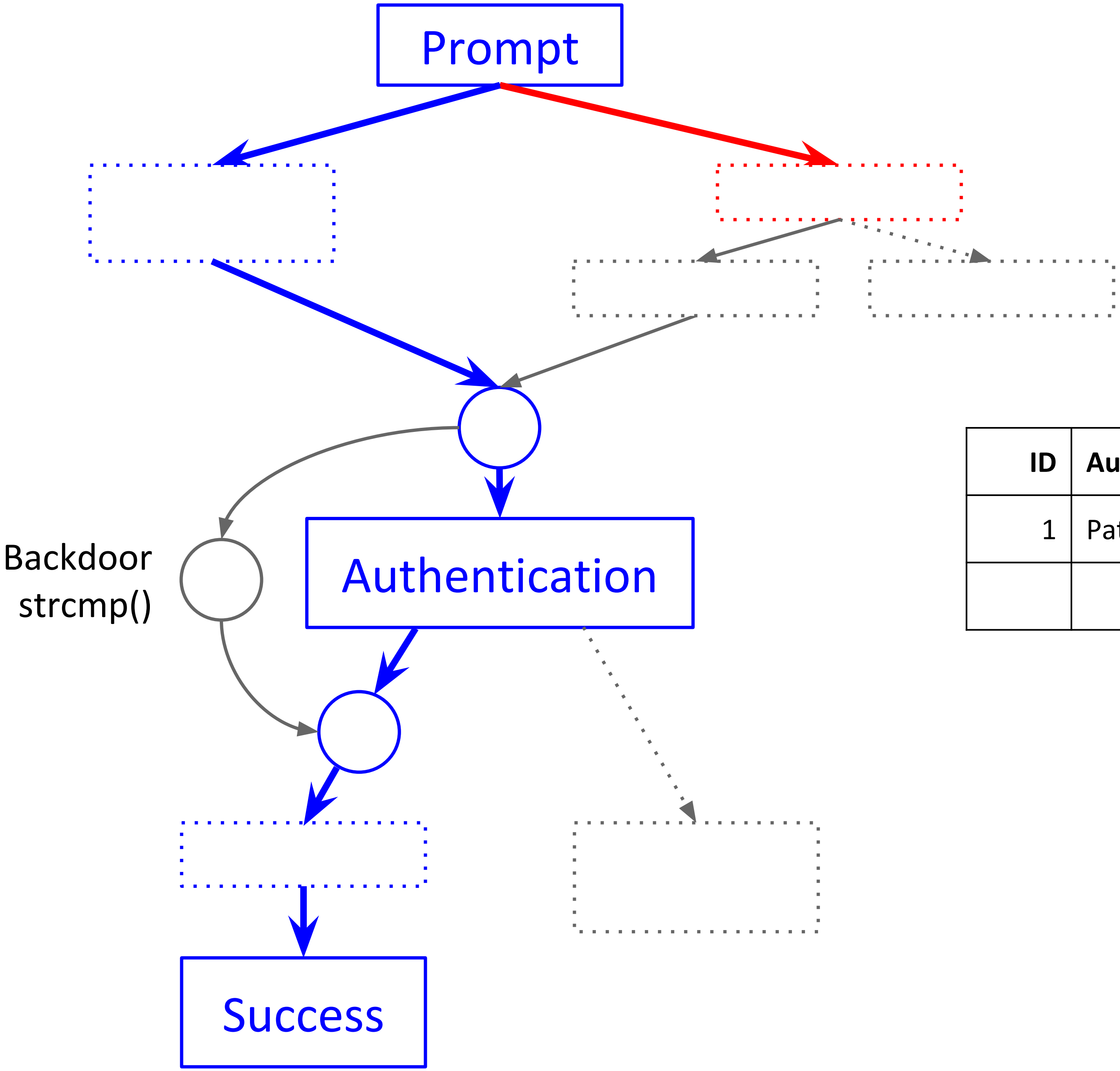
ID	Authenticated Paths
1	Path 1

Step 7



ID	Authenticated Paths
1	Path 1

Path 1



Prompt

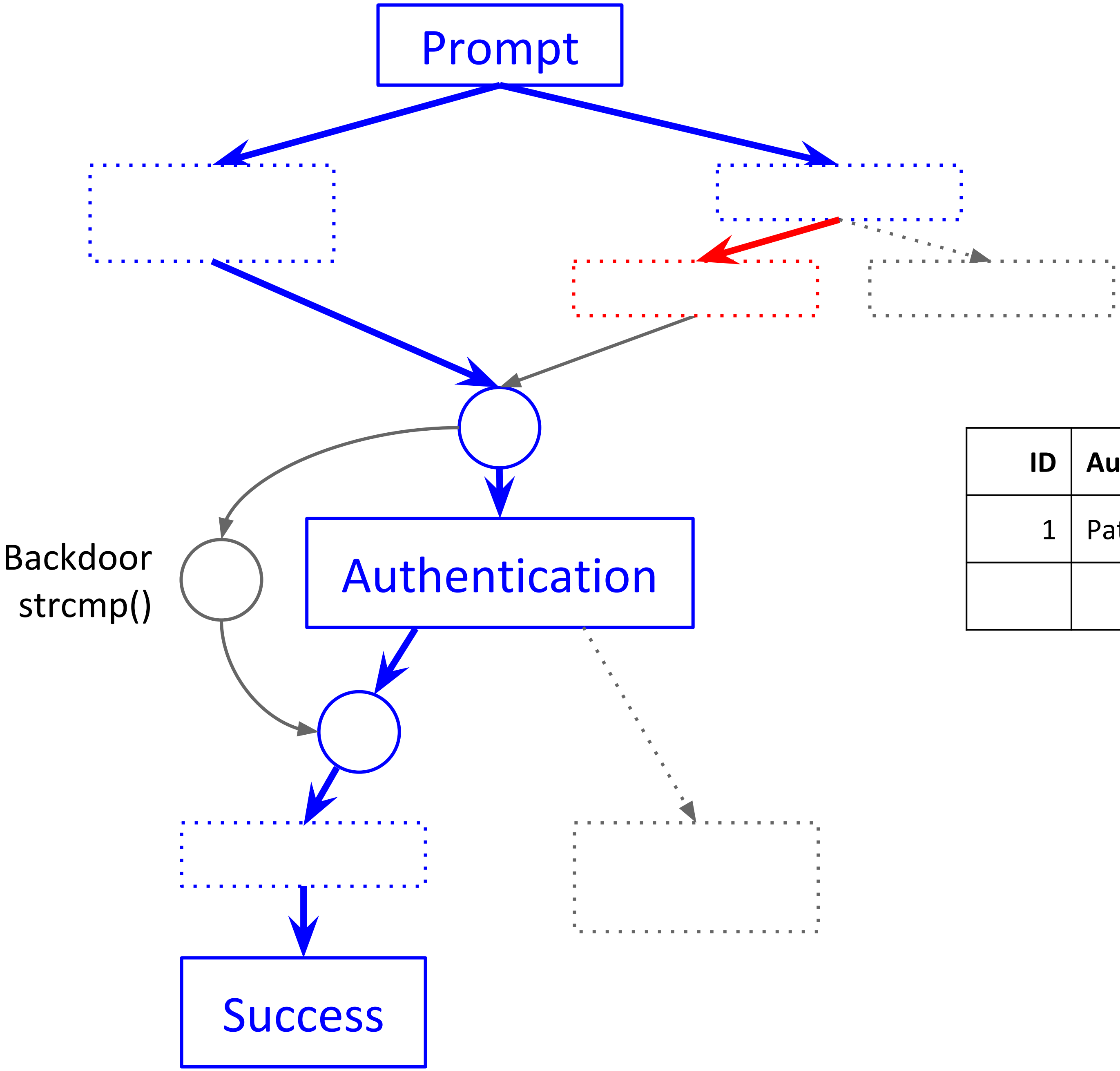
Backdoor
strcmp()

Authentication

Success

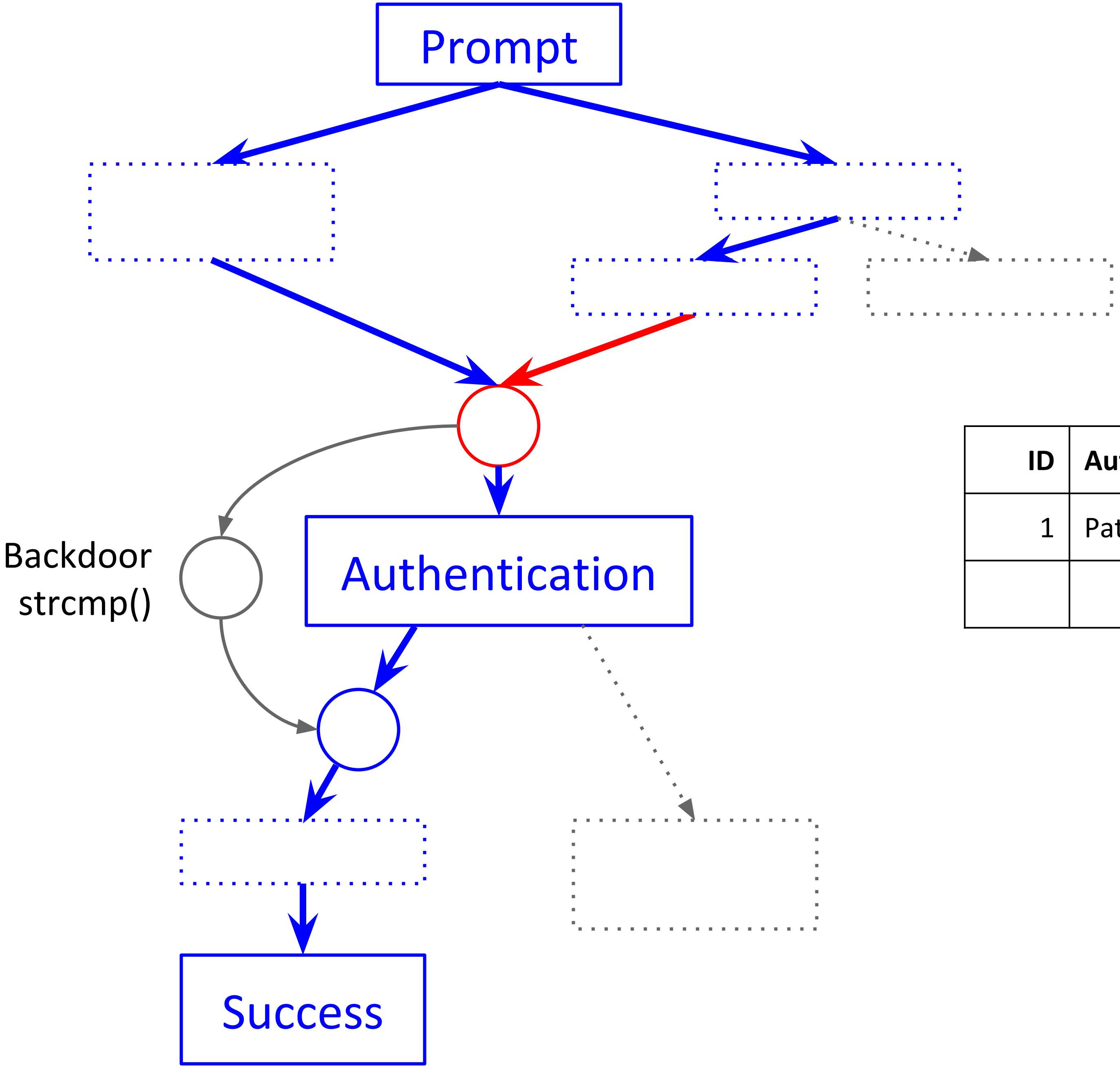
ID	Authenticated Paths
1	Path 1

Step 8



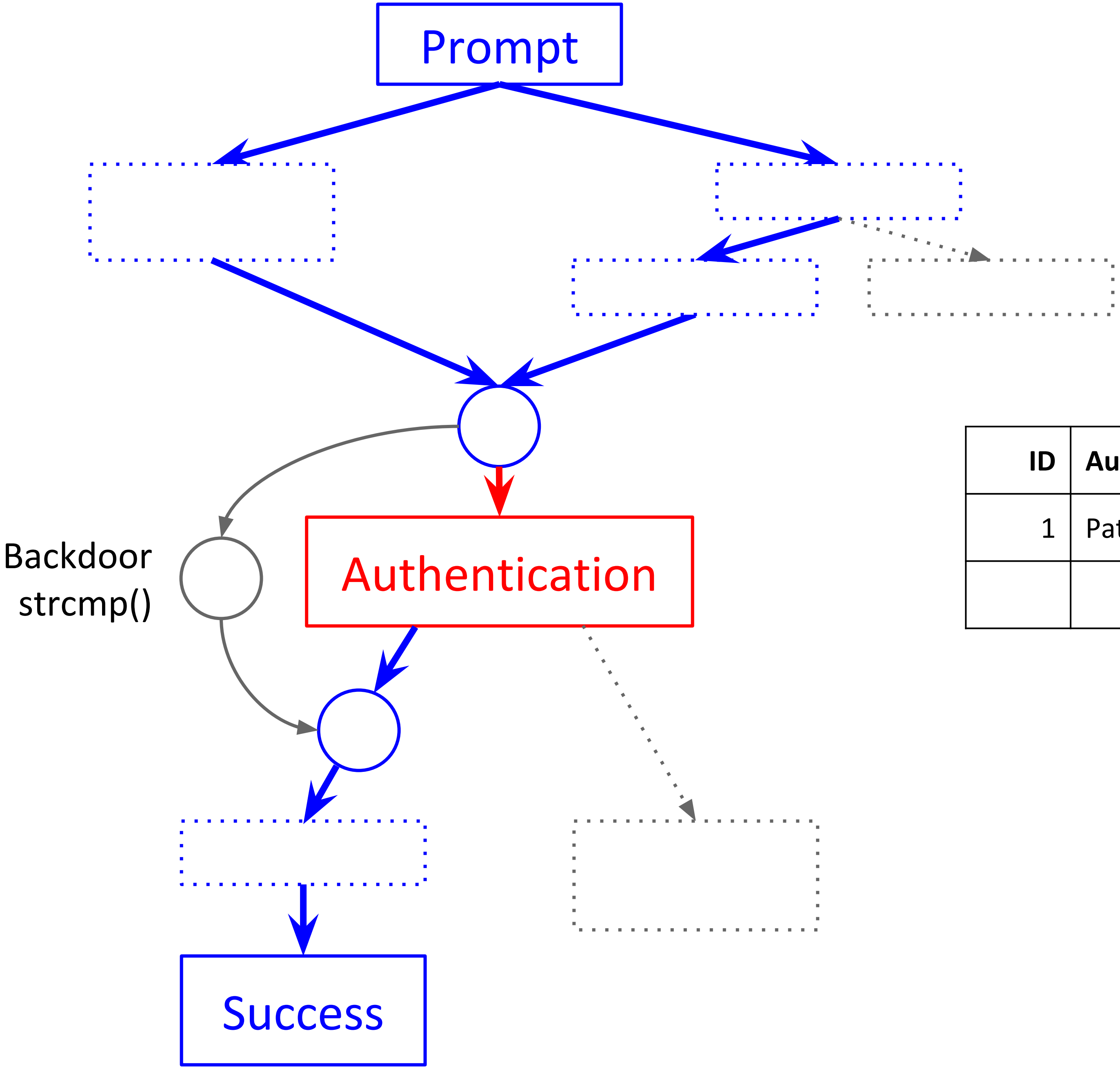
ID	Authenticated Paths
1	Path 1

Step 9



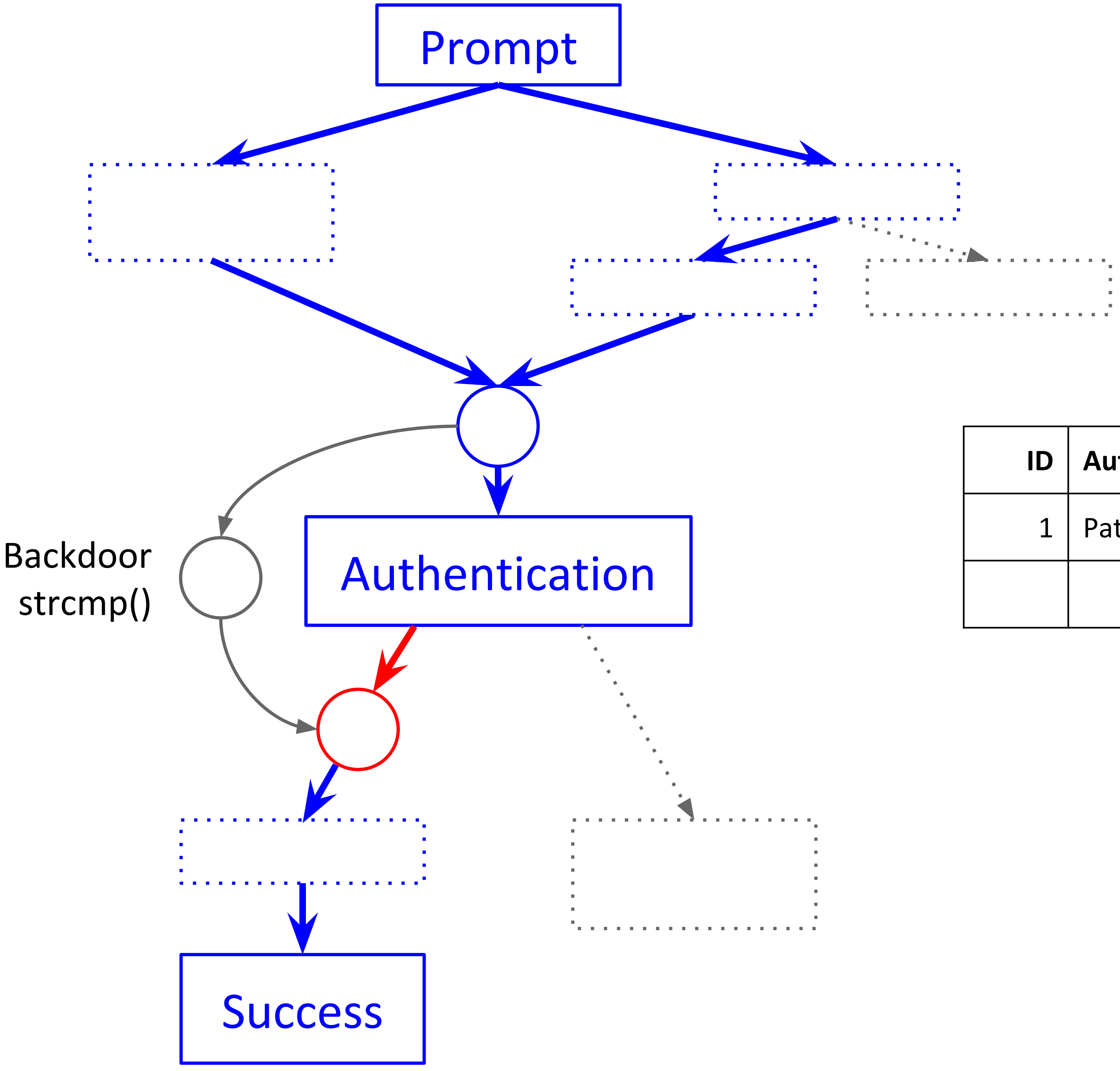
ID	Authenticated Paths
1	Path 1

Step 10



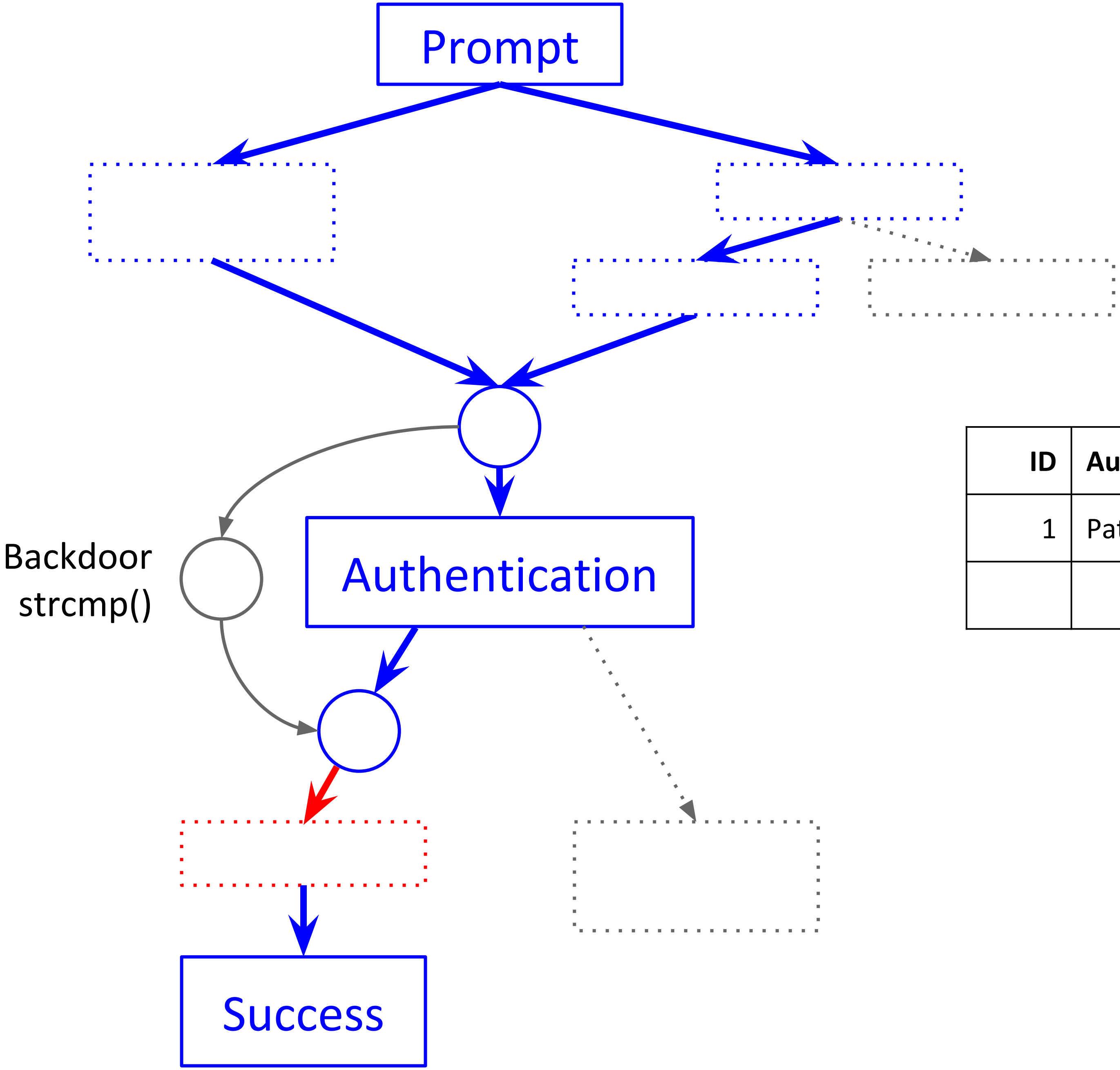
ID	Authenticated Paths
1	Path 1

Step 11



ID	Authenticated Paths
1	Path 1

Step 12



Prompt

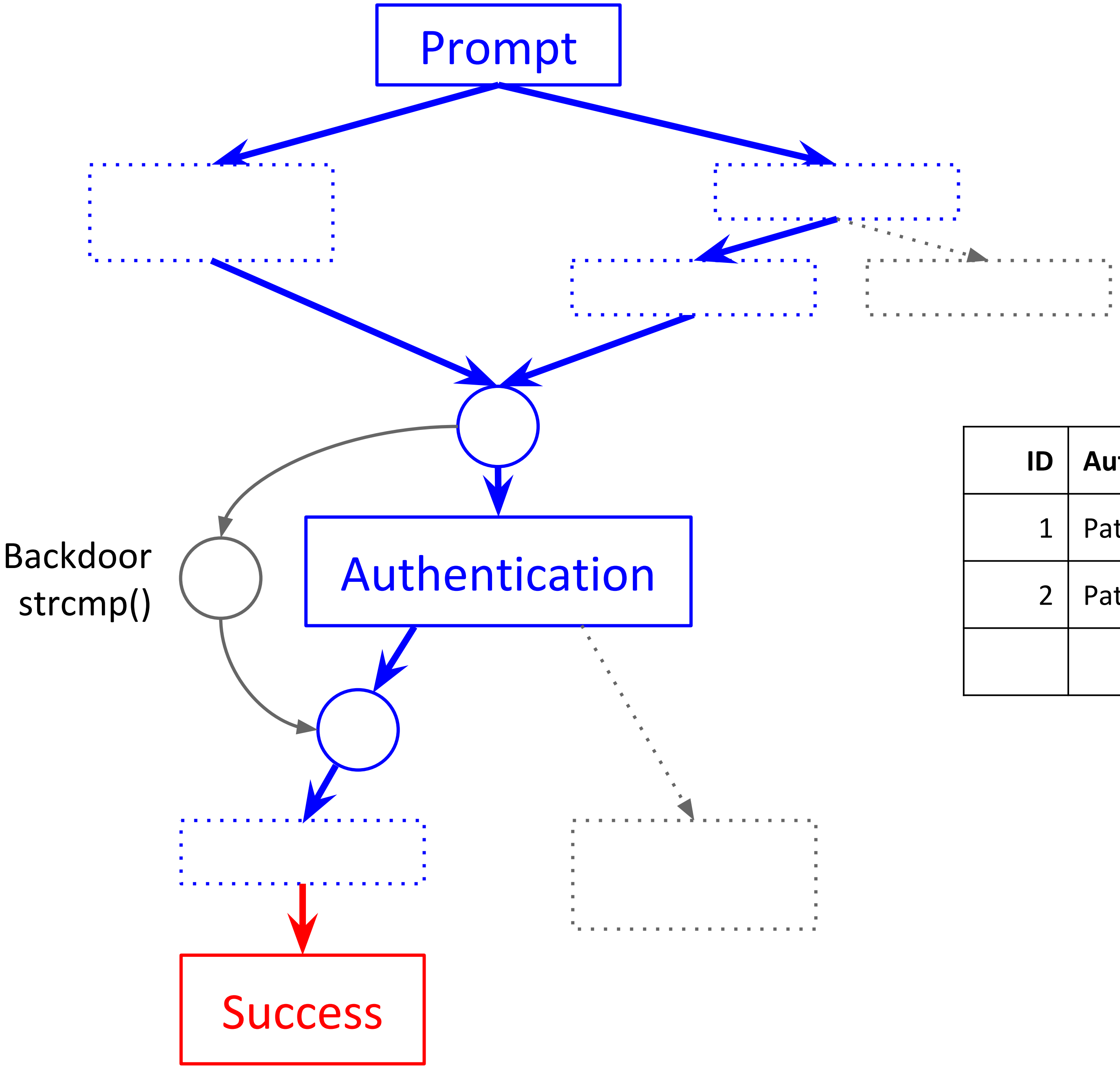
Backdoor strcmp()

Authentication

Success

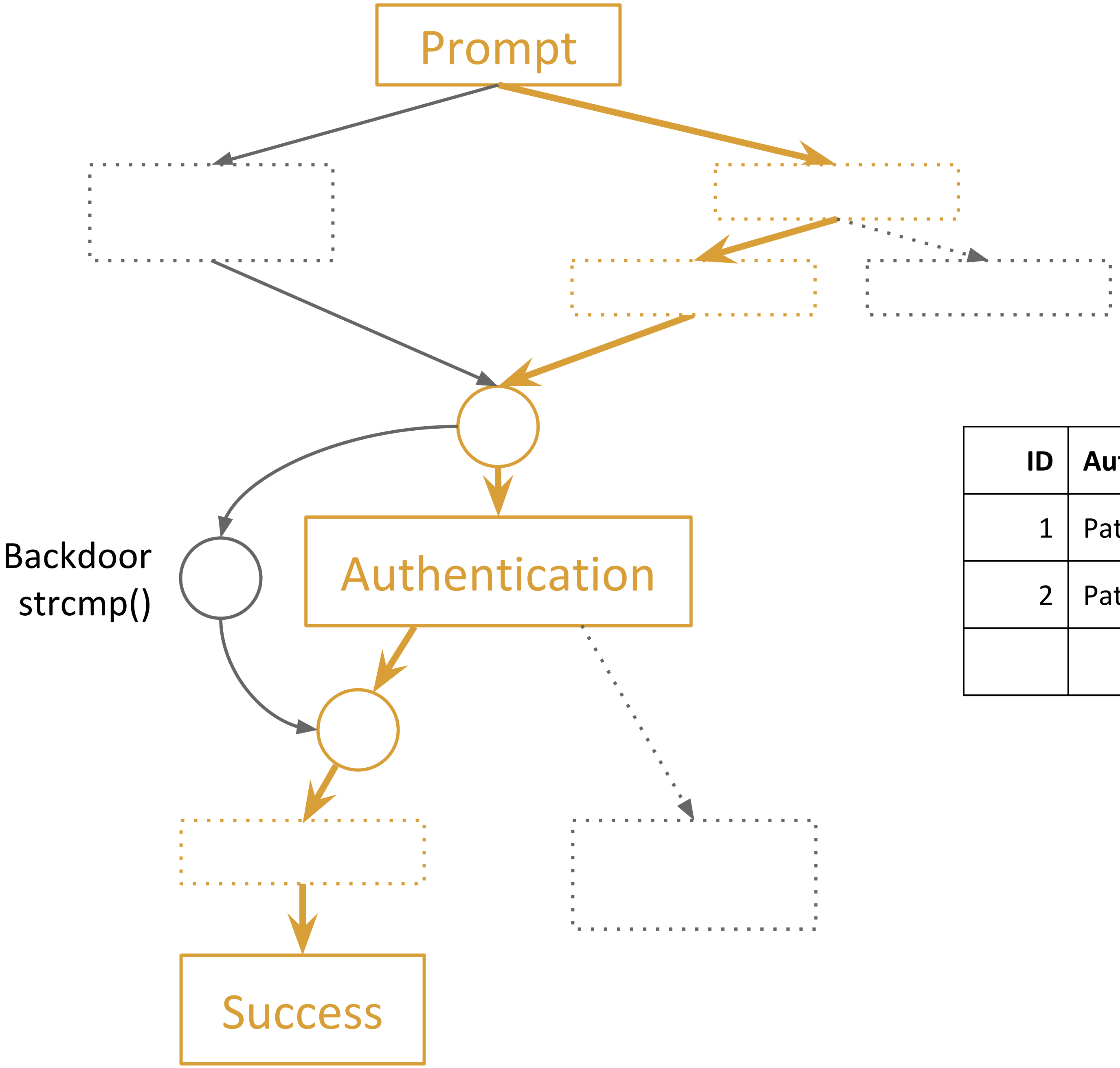
ID	Authenticated Paths
1	Path 1

Step 13



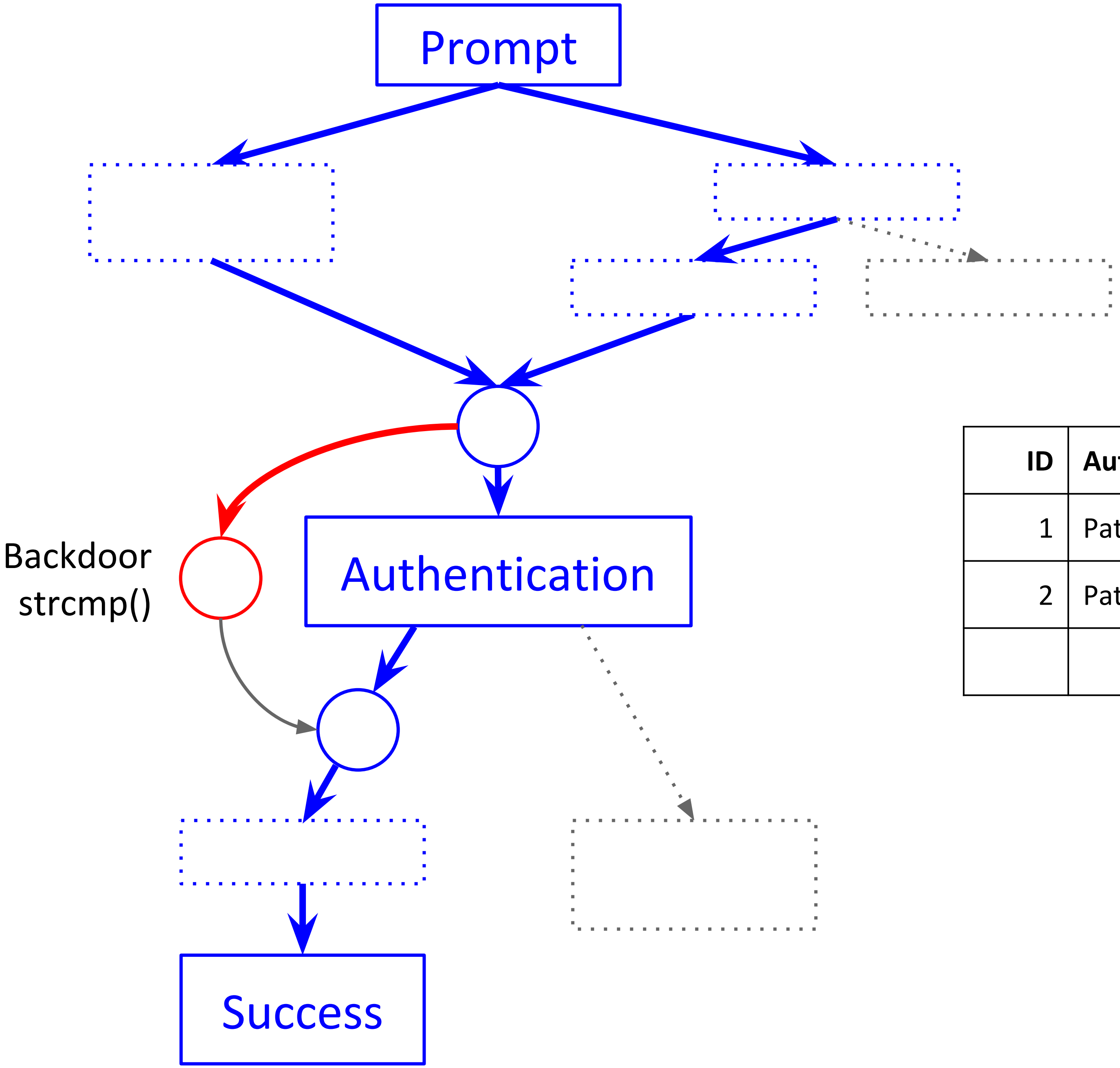
ID	Authenticated Paths
1	Path 1
2	Path 2

Step 14



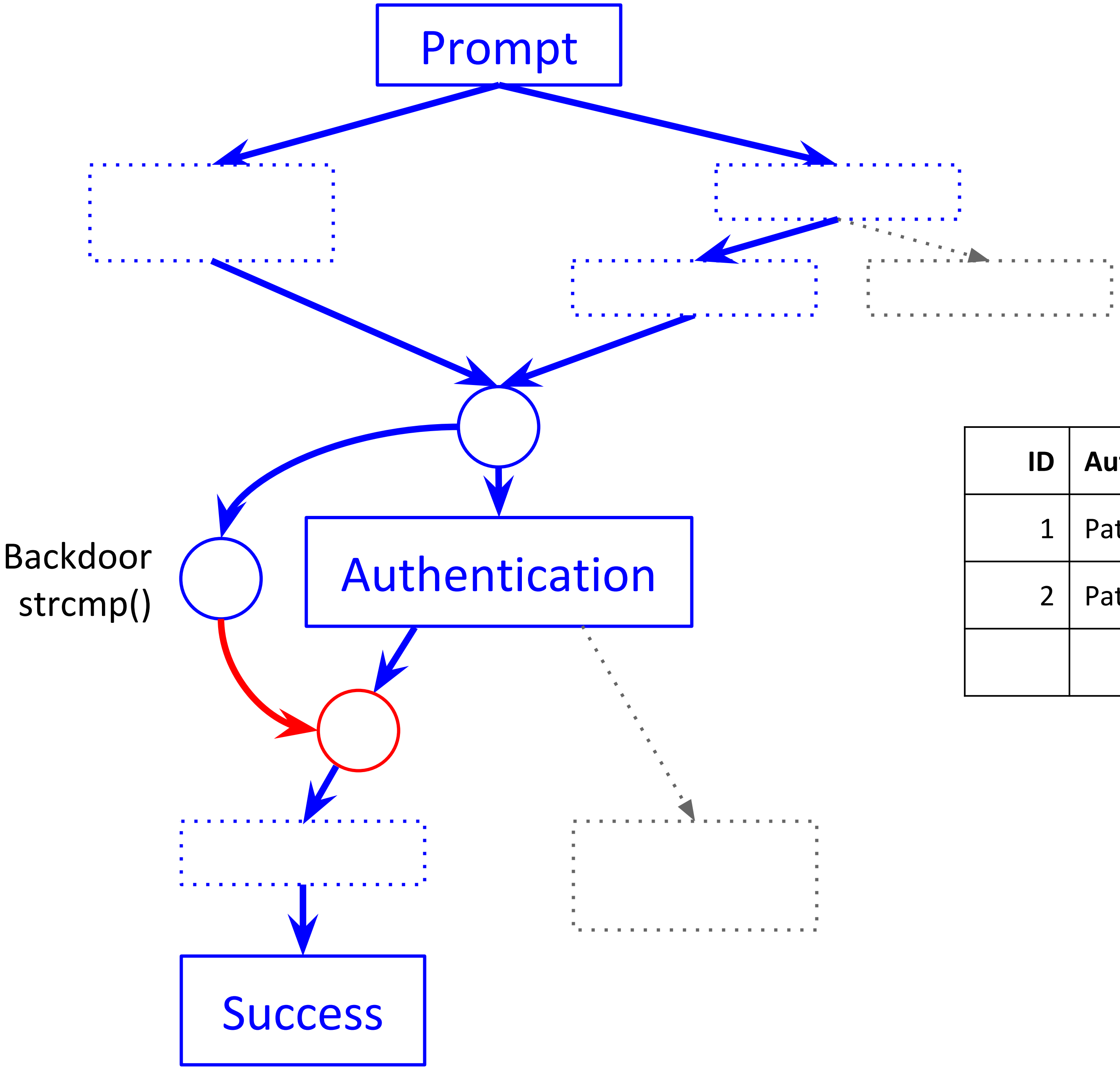
ID	Authenticated Paths
1	Path 1
2	Path 2

Path 2



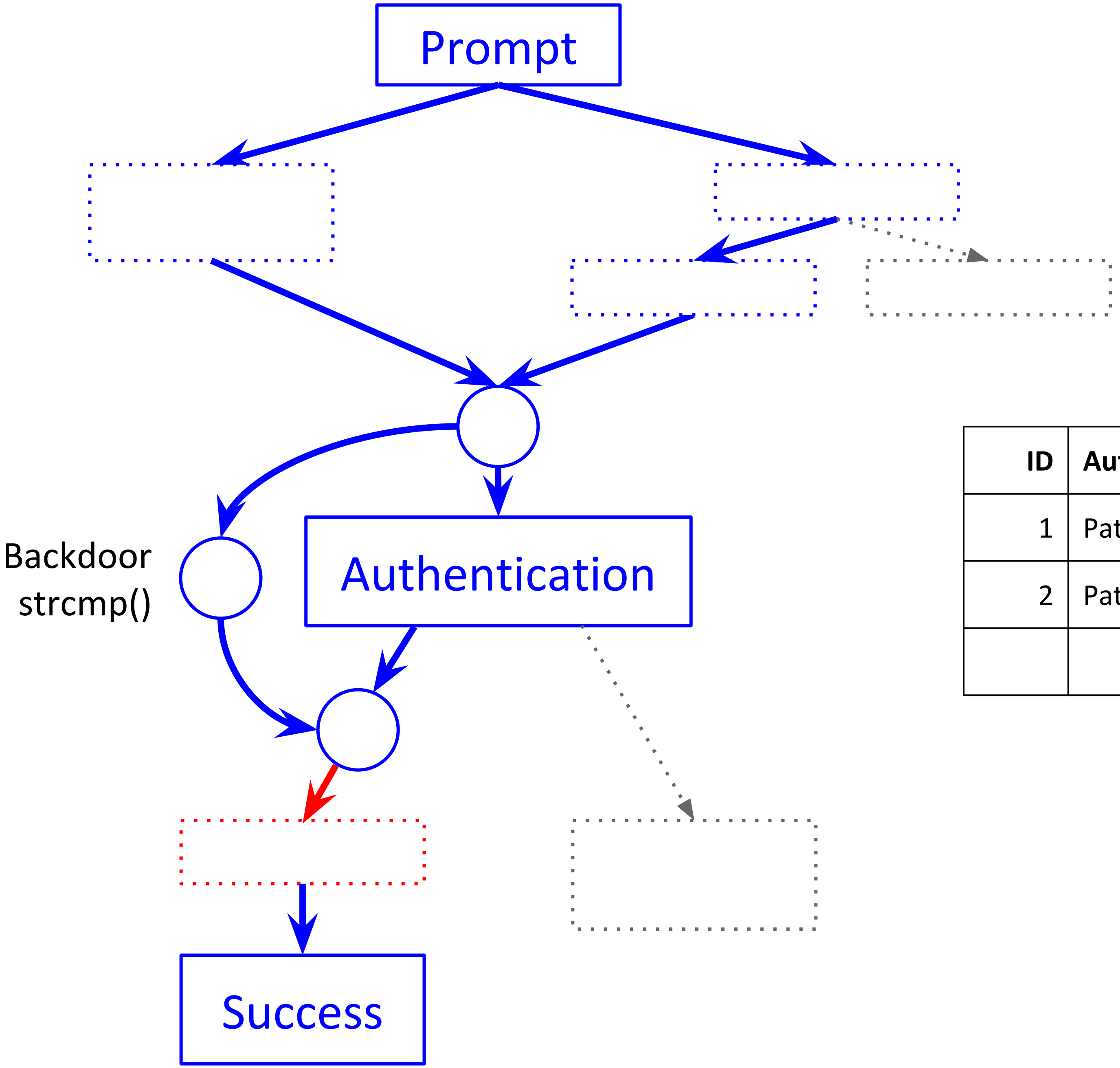
ID	Authenticated Paths
1	Path 1
2	Path 2

Step 15



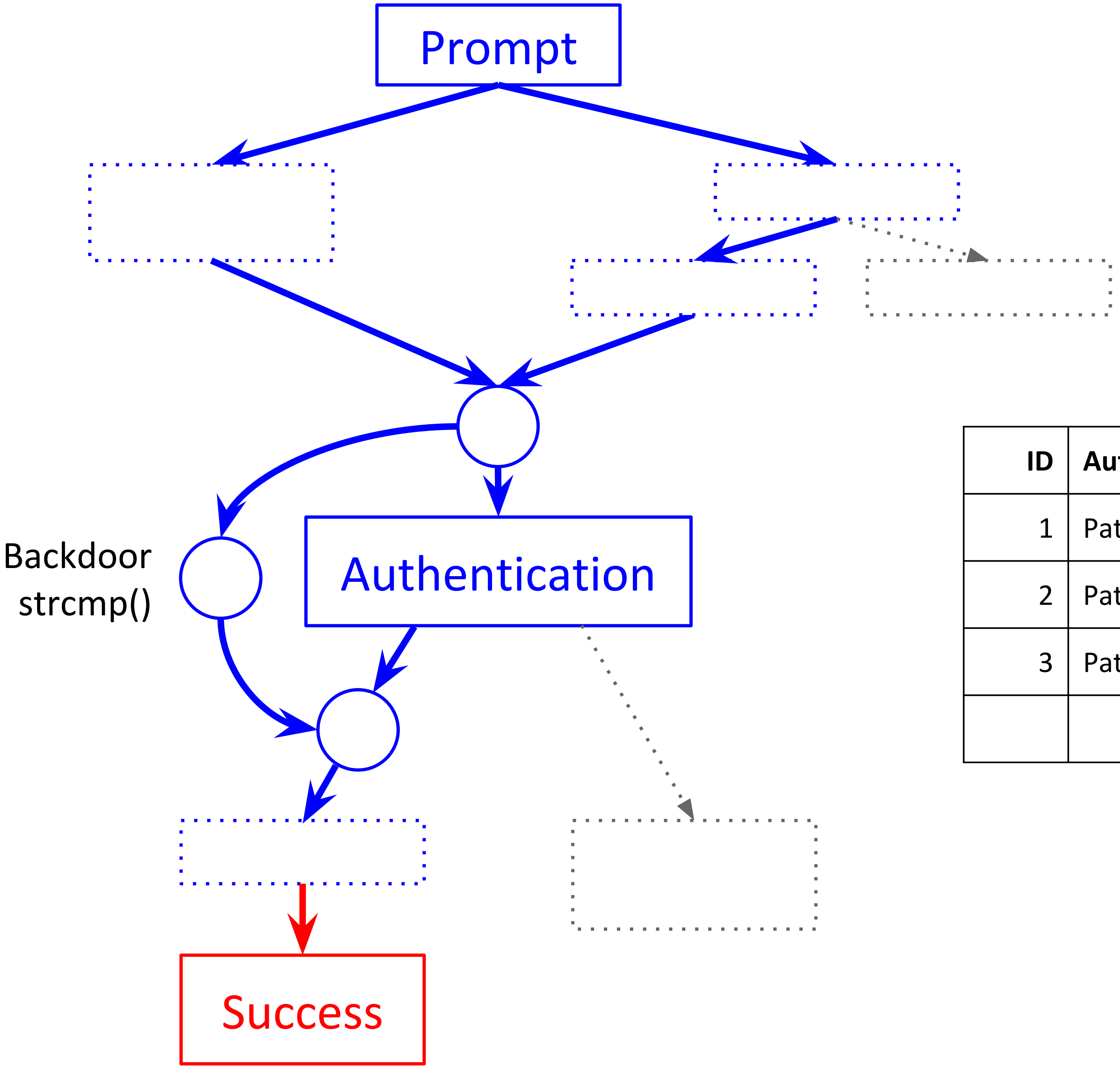
ID	Authenticated Paths
1	Path 1
2	Path 2

Step 16



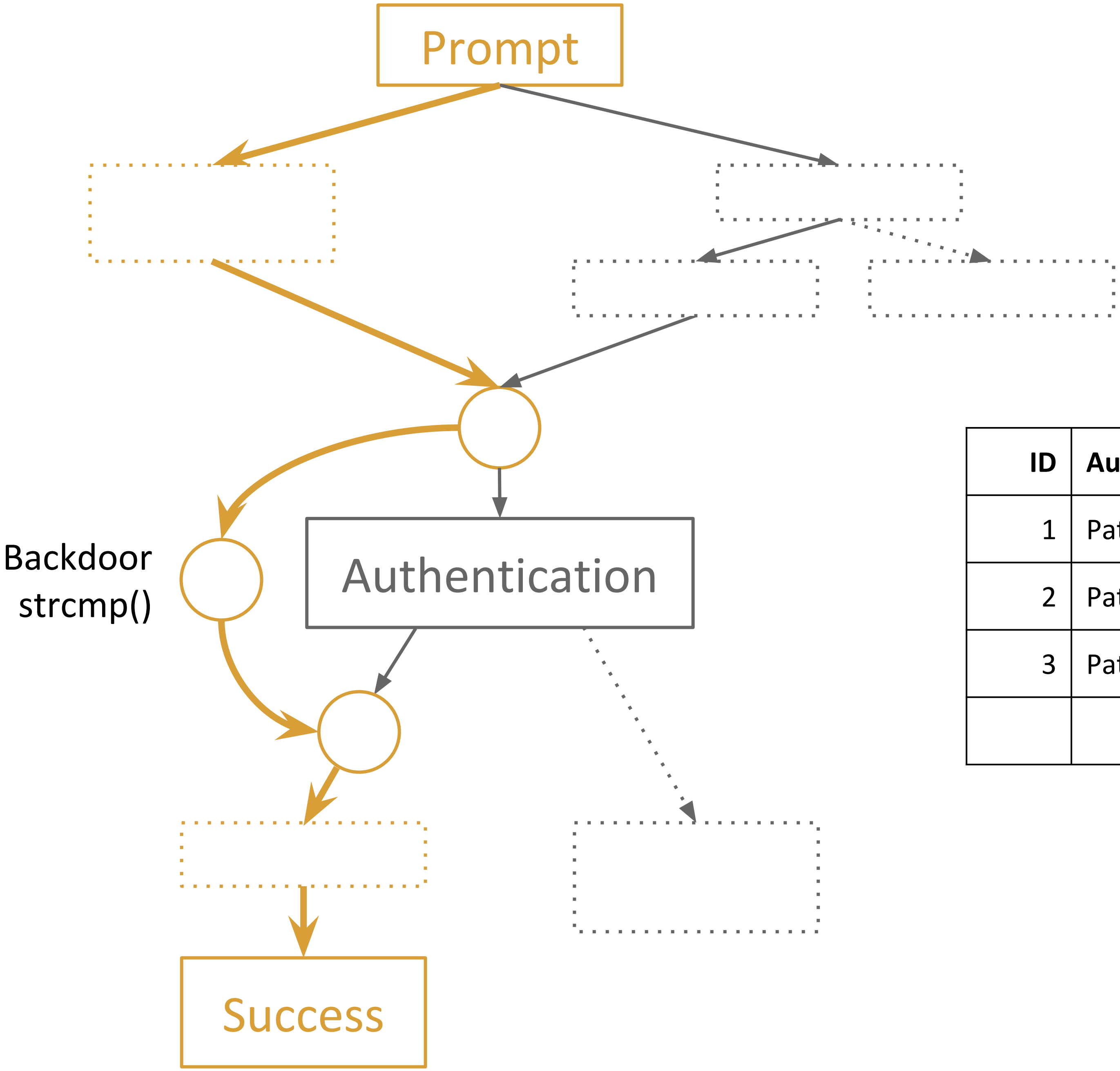
ID	Authenticated Paths
1	Path 1
2	Path 2

Step 17



ID	Authenticated Paths
1	Path 1
2	Path 2
3	Path 3

Step 18



Prompt

Backdoor
strcmp()

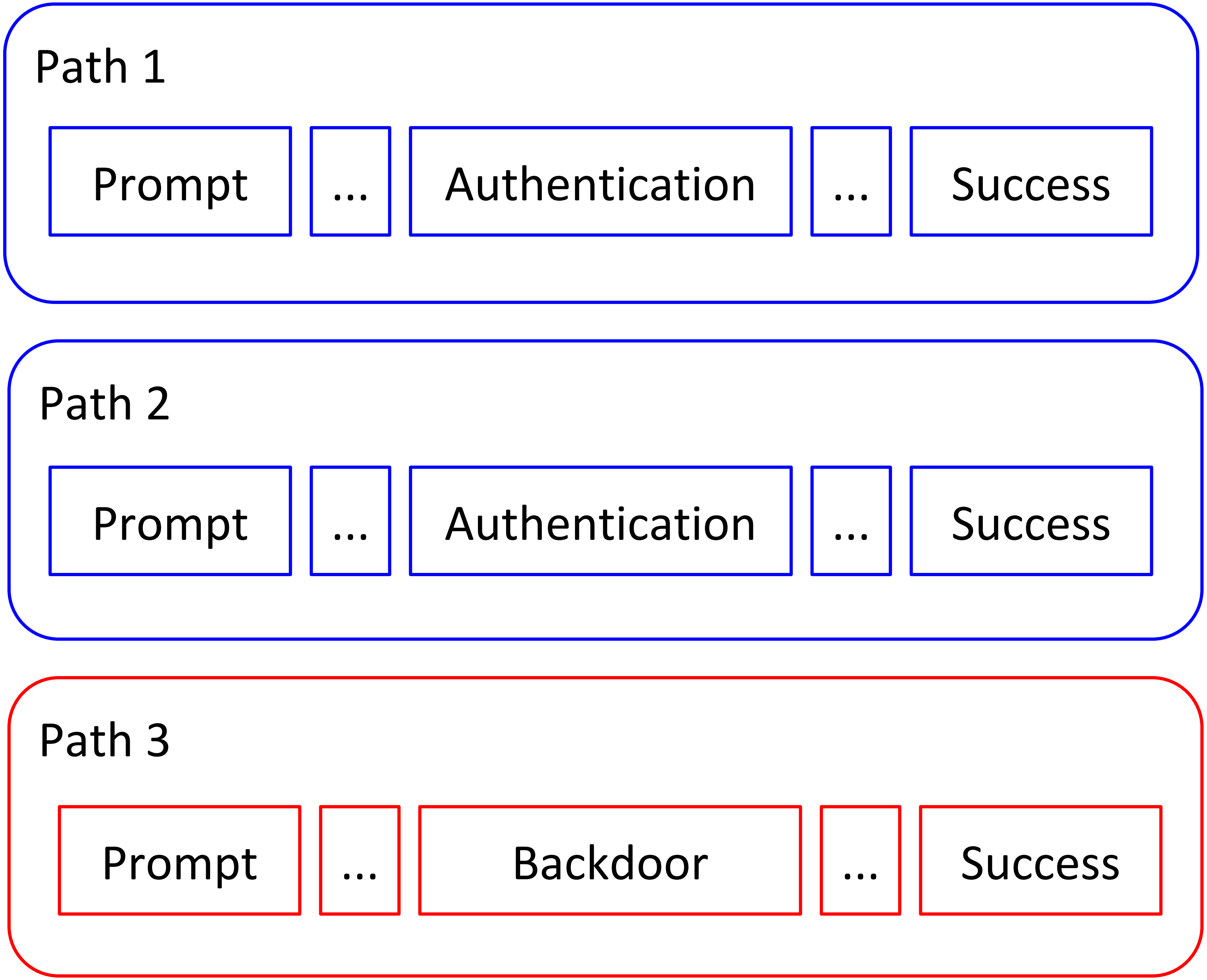
Authentication

Success

ID	**Authenticated Paths**
1	Path 1
2	Path 2
3	Path 3

Path 3

Authentication Bypass



Path 1

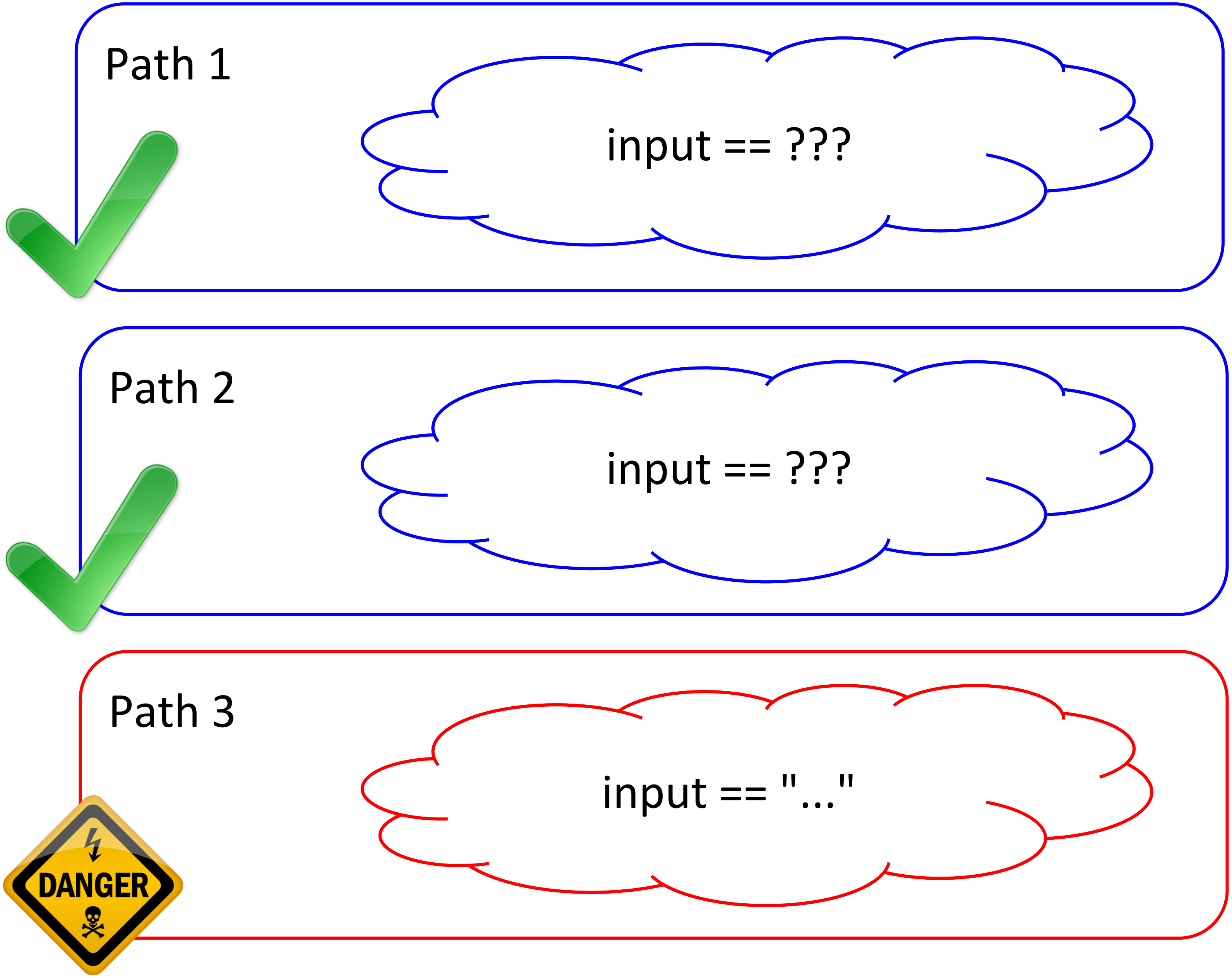
Prompt … Authentication … Success

Path 2

Prompt … Authentication … Success

Path 3

Prompt … Backdoor … Success



Path 1

input == ???

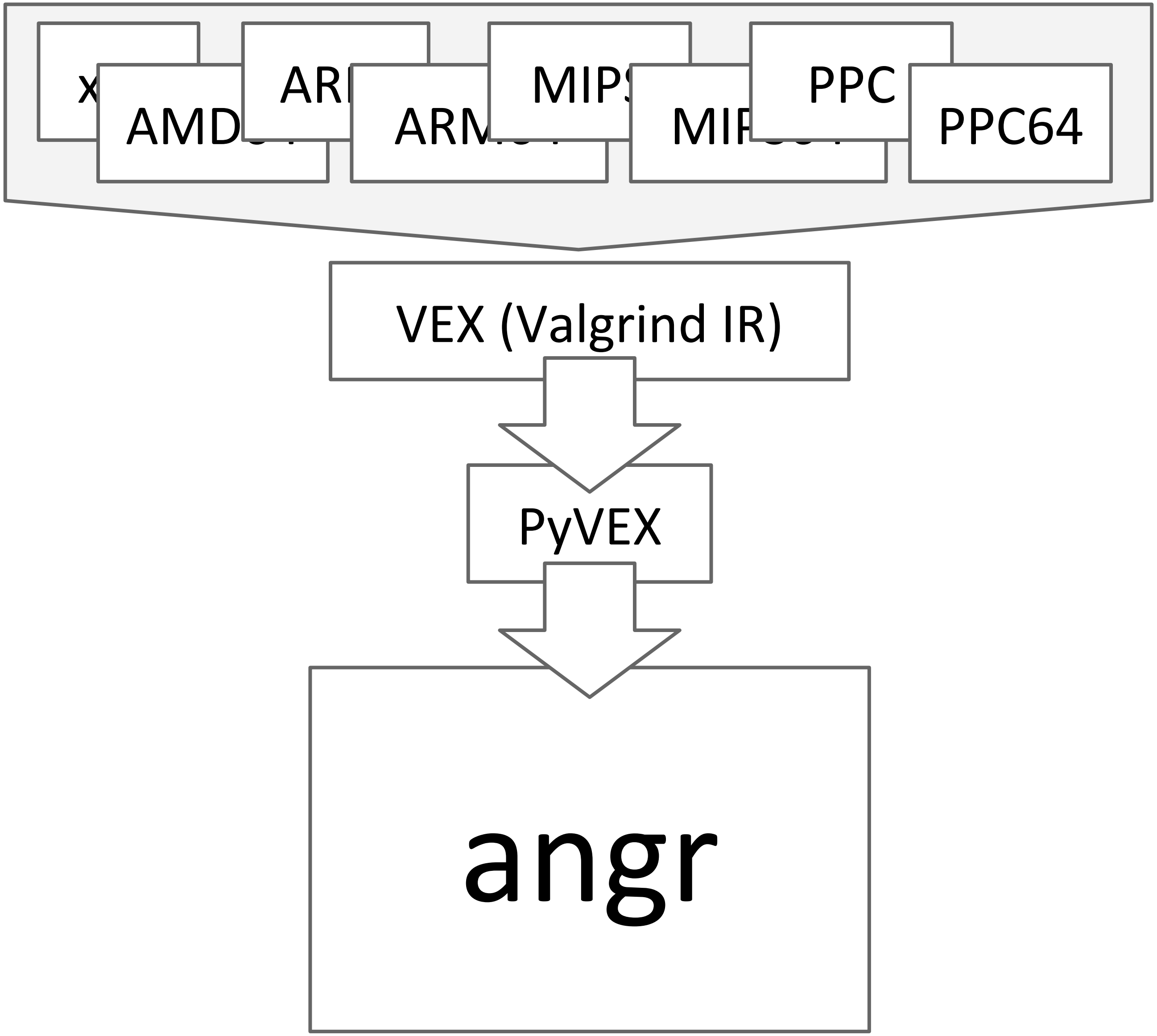
Path 2

input == ???

Path 3

input == "..."

Implementation Details



x

AMD

AR

ARM

MIPS

MIP

PPC

PPC64

VEX (Valgrind IR)

PyVEX

angr

Backdoor Example

3S Vision N5072

Linux embedded device.

HTTP server for management and video monitoring.

Security Policy

- → Authentication required for footage access
- → "Image-Type" header

Backdoor

- → Hard-coded user credentials
- → Username: 3sadmin
- → Password: 27988303

Slicing

- → 5m
- → 212 bb

DSE

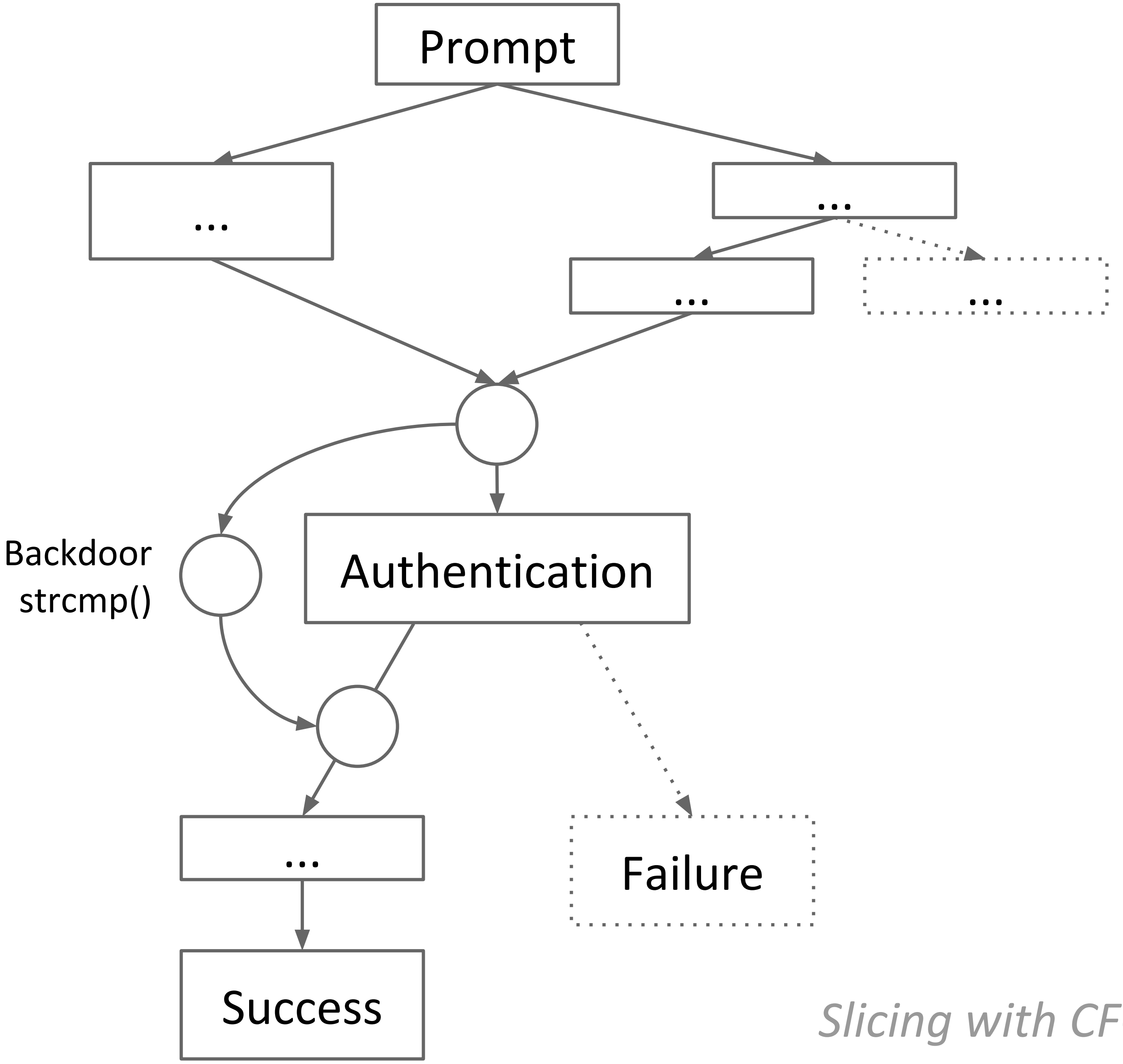
- → 26m

Summary

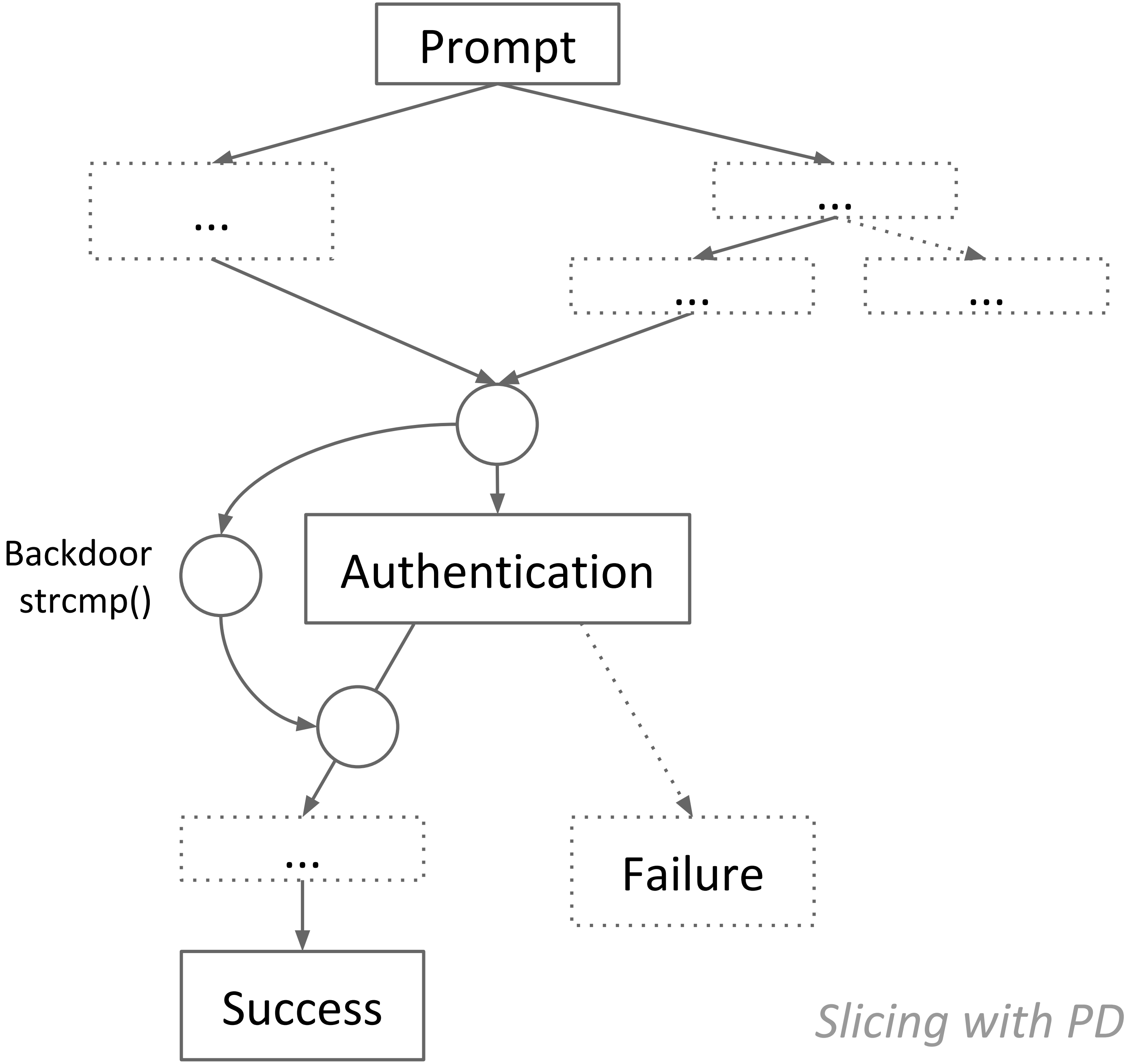
➔ New backdoor model: *input determinism*

➔ Implemented analysis system

➔ Found backdoors in real firmware!



Slicing with CFG



Slicing with PDG

Dell 1130n

Modified VxWorks system.

Includes an SNMP daemon for monitoring and management.

Security Policy

- ➔ Manually identified sensitive memory regions

Backdoor

- ➔ Specific SNMPv1 community string would allow configuration without checking authentication

Slicing

- ➔ 14m
- ➔ 532 bb

DSE

- ➔ >11h