University of Massachusetts Amherst

COUNTERFOIL: Verifying Provenance of Integrated Circuits using Intrinsic Package Fingerprints and Inexpensive Cameras

USENIX Security '20

Siva Nishok Dhanuskodi

Xiang Li

Daniel E. Holcomb

University of Massachusetts Amherst

sdhanusk@umass.edu

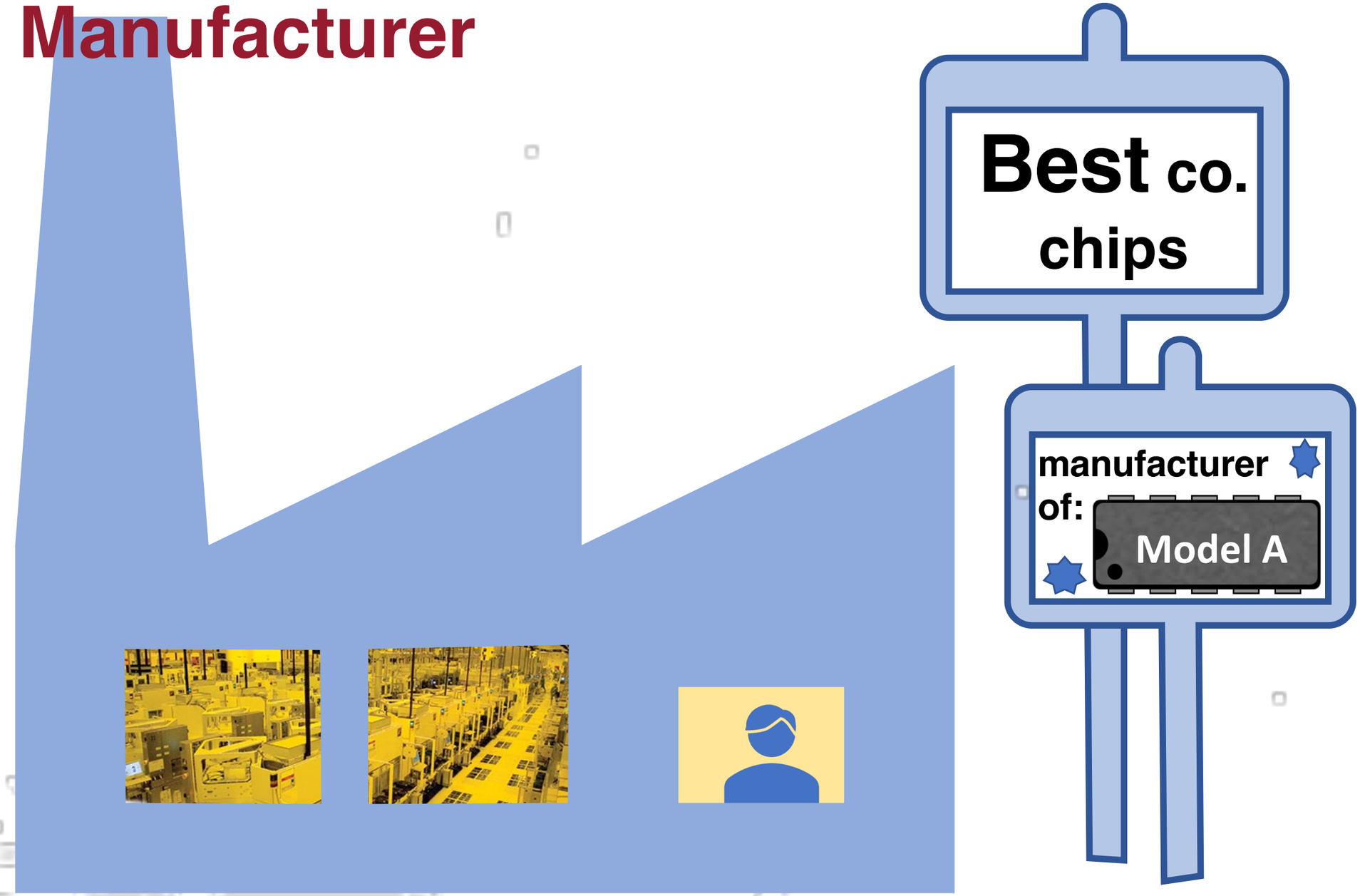
Global semiconductor market is $500B/year
Estimated $5B/year lost to counterfeiting[1]

CounterFoil: A practical low-cost scheme to verify provenance

[1]Kae-Nune and Desseguier, 2013

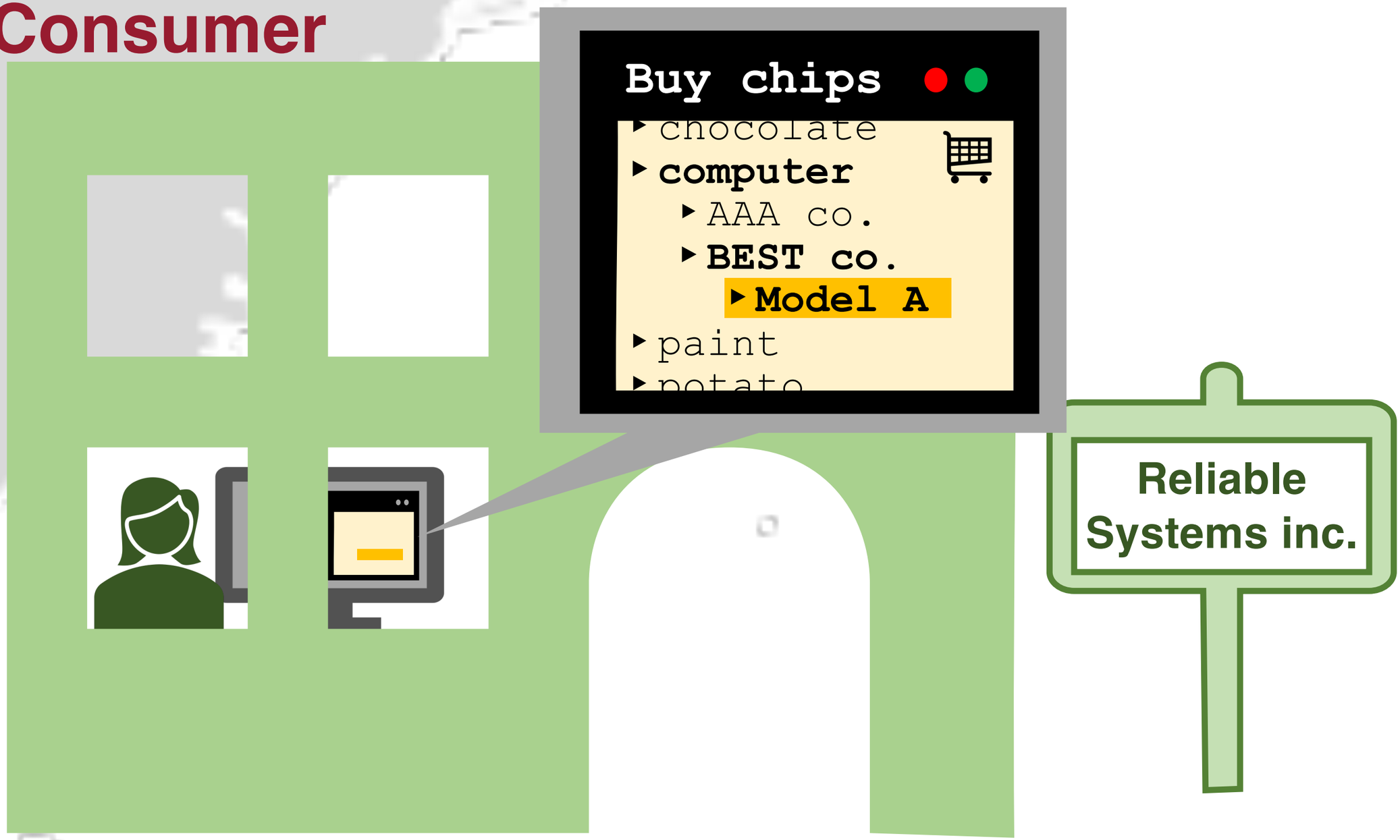
Global Distribution Network

Manufacturer

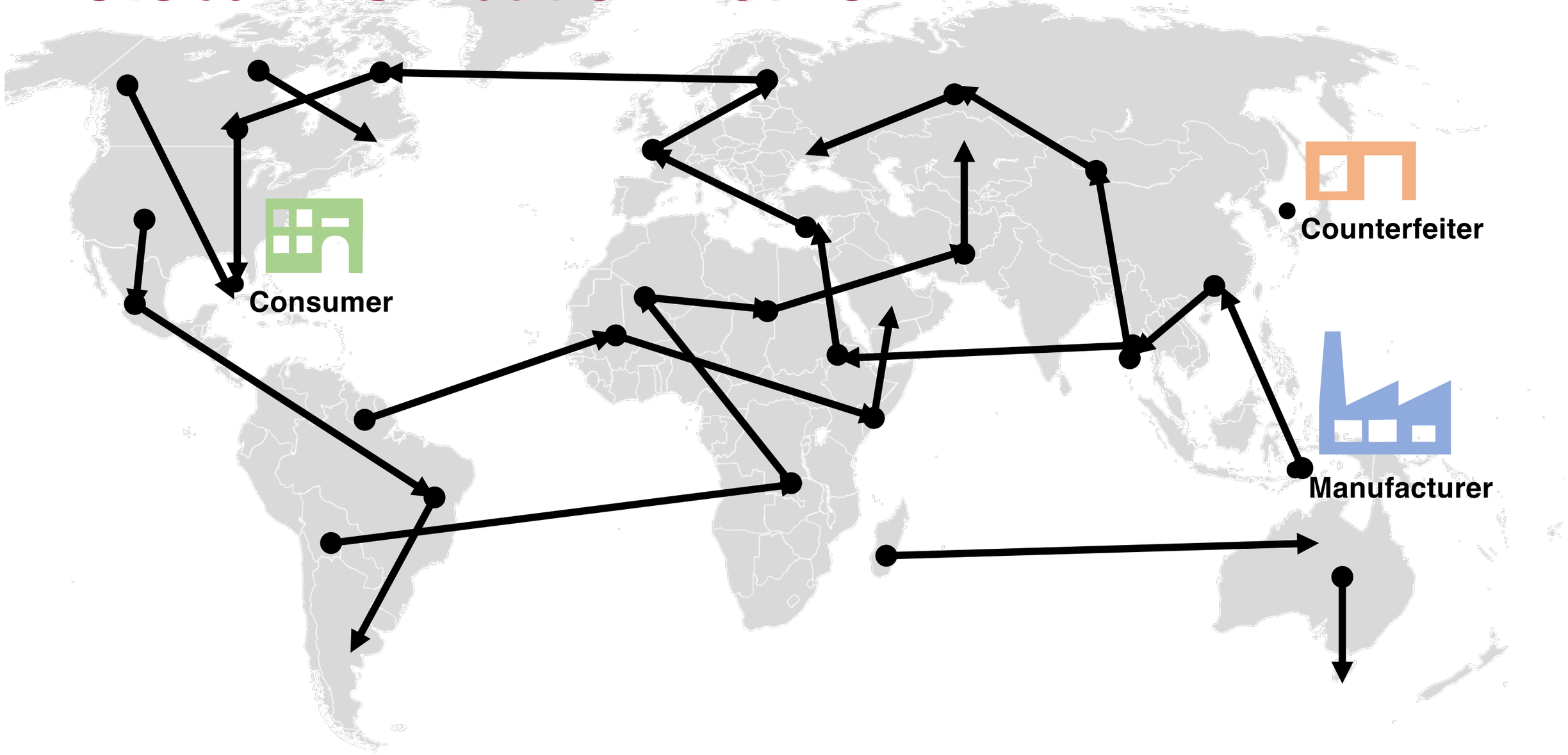


Global Distribution Network

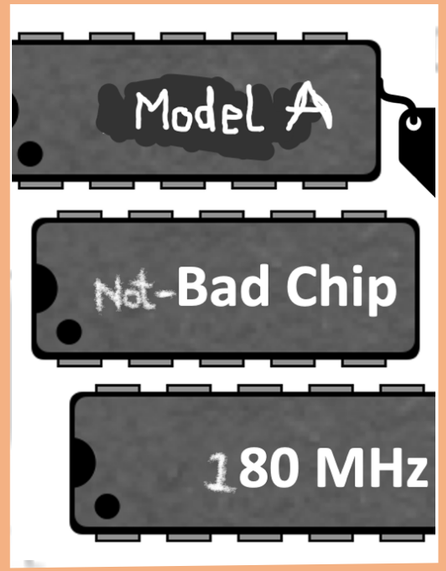
Consumer


Buy chips
chocolate
computer
AAA co.
BEST co.
Model A
paint
potato
Reliable Systems inc.

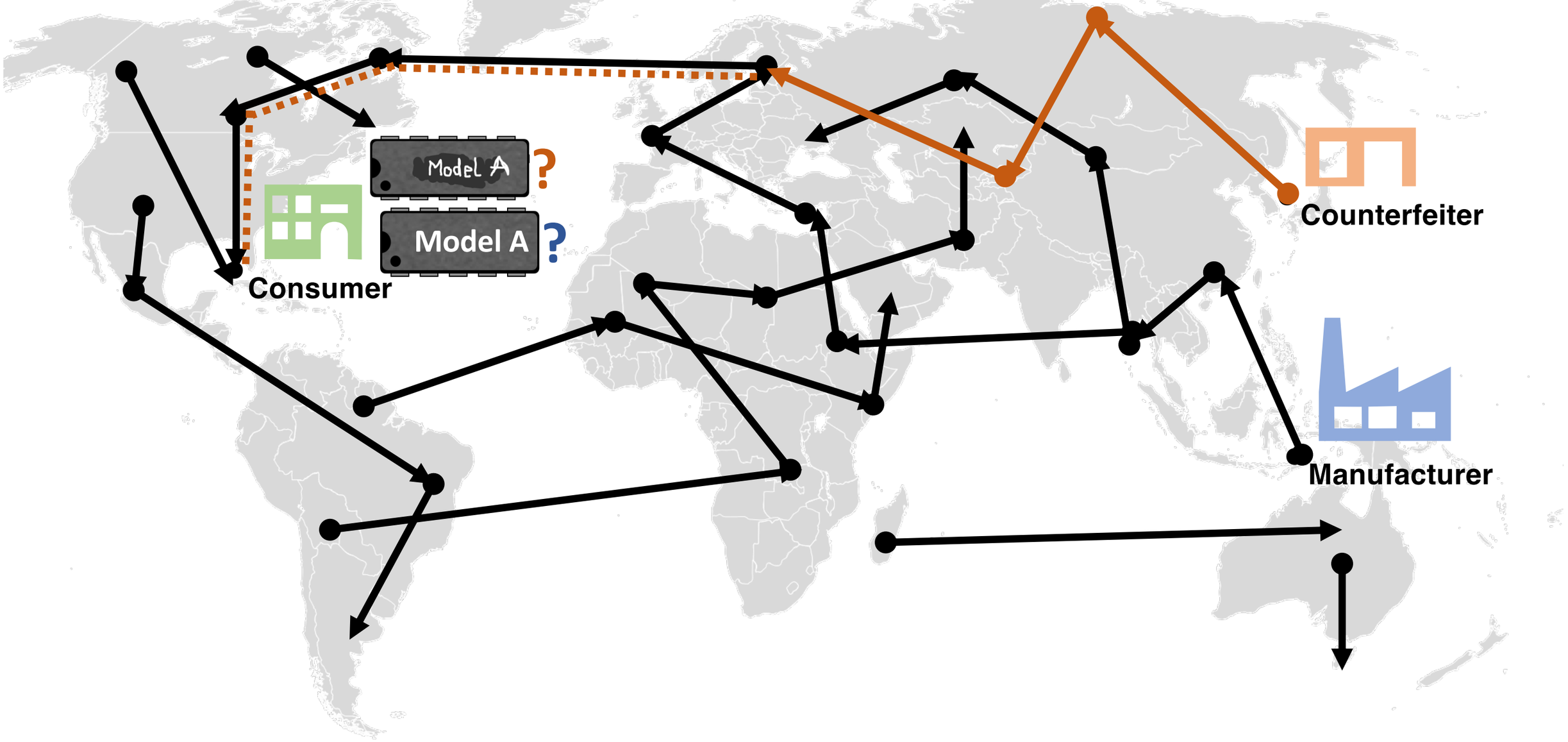
Global Distribution Network



Counterfeiter



Global Distribution Network



CNNMoney
A Service of CNN, Fortune & Money

FORTUNE | Money

Home | Video | Business News | Markets | My Portfolio | Investing | Economy | Tech | Personal

Brainstorm Tech | Mobile | Security | Social | Innovation | Enterprise | Apple 2.0 | Tech30 | Interactiv

THE CYBERCRIME ECONOMY

Fake tech gear has infiltrated the U.S. government

Starlino electronics

HOME ARTICLES

FTDI chip real of fake ? How to spot a fake RT232R / RT232RL and others ?

POSTED ON NOVEMBER 12, 2015 BY STARL

ICE

TO REPORT CRIMES: EMAIL OR C

Home | About ICE | Investigations | National Security | Enforcement & Removal

News Room » Recent Releases

- Recent Releases
- Library
- Images and Videos
- Legal Notices
- Media Kit
- Widgets

Find releases based on

Location (State)...

Month...

Topic...

News Releases

NOVEMBER 19, 20

Guilty plea in co
Counterfeit integ

WASHINGTON - T
scheme in which s
contractors and oth
Customs Enforcem
federal agencies.

Stephanie A. McCl
to a charge of cons
a three-year term o
U.S. sentencing gu
been scheduled.

sparkfun START SOMETHING

SHOP | LEARN | BLOG | SUPPORT

PRODUCT MENU | find products, tutorials, etc...

HOME / BLOG / 2010.05.17

Revisiting the Counterfeit ATMega328s

A SparkFun customer and a a local dentist investigate the ATMega328 "slugs" - with interesting findings.

BY EMCEE GRADY MAY 17, 2010 02:00 EDT 41 BUSINESS TEARDOWN

on of the story is that we got some
etting a microcontroller running?

on the right.

The Washington Post

In the News | Condoleezza Rice | Floyd Mayweather | Ukraine | Kentucky Derby | WHCD

washingtonpost.com > Metro > Crime

3 in Calif. Accused of Selling Counterfeit Computer Circuits

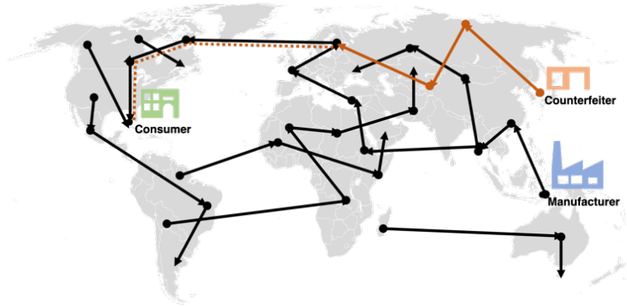
By Del Quentin Wilber
Washington Post Staff Writer
Saturday, October 10, 2009

TOOLBOX

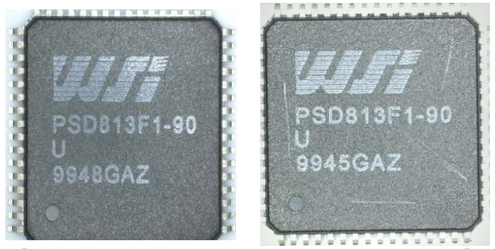
Resize | Print | E-mail | Reprints

dvisory
as

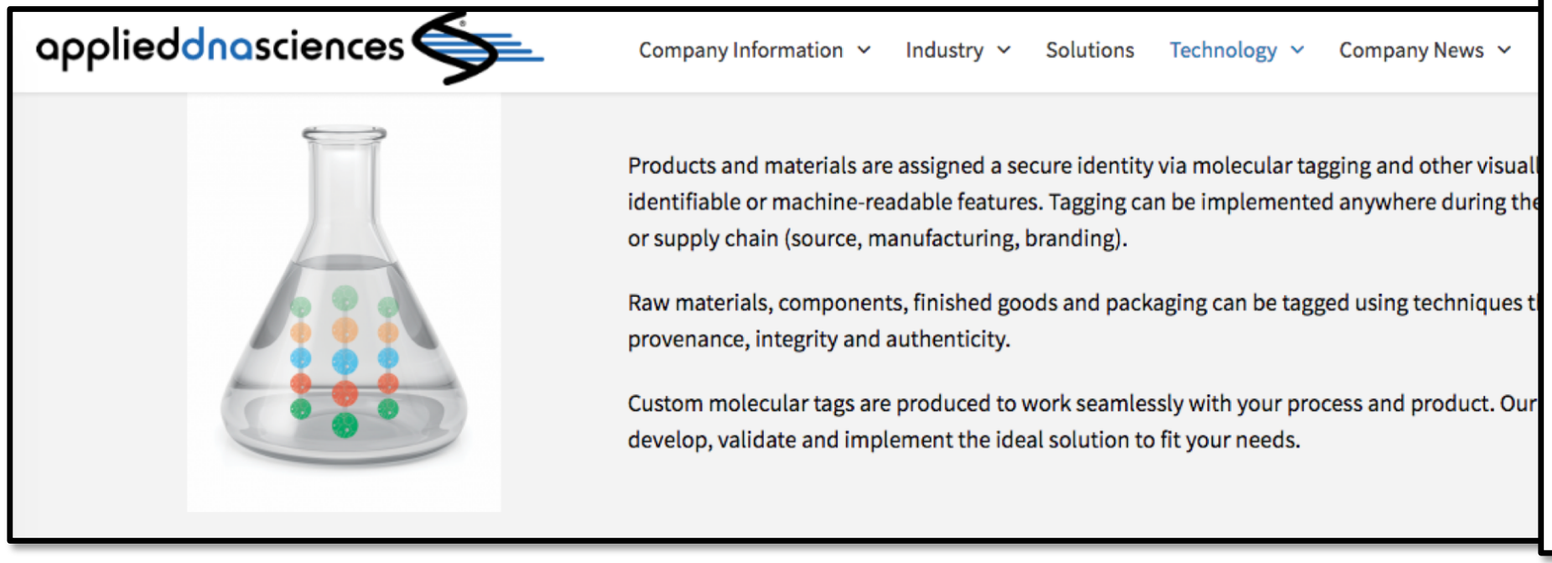
Countermeasures



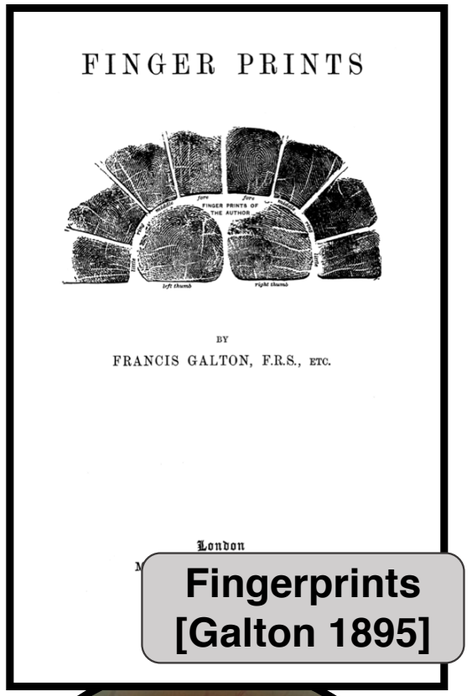
- Anomaly detection
  - Look for something unusual
  - E.g. Visual inspection, classification, electronic signatures
- Authenticate provenance
  - Look for something you trust



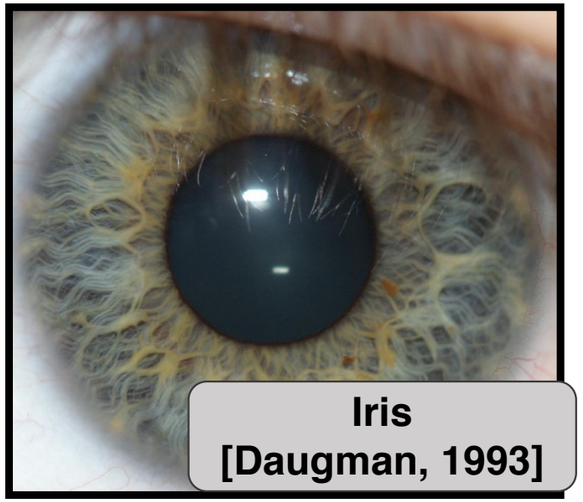
[Asadizanjani et al., ISTFA 2016]



Biometrics



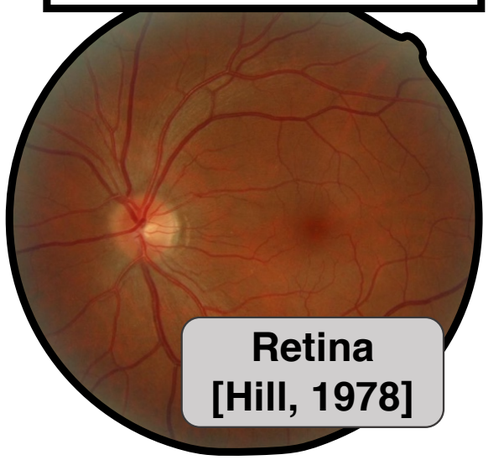
Fingerprints
[Galton 1895]



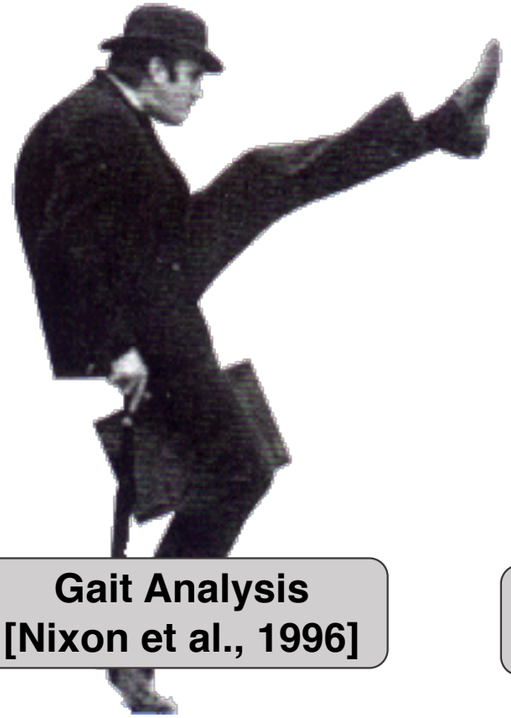
Iris
[Daugman, 1993]

Ear shape
[Choras et al., 2004]

Compact Discs
[Hammouri et al., 2009]

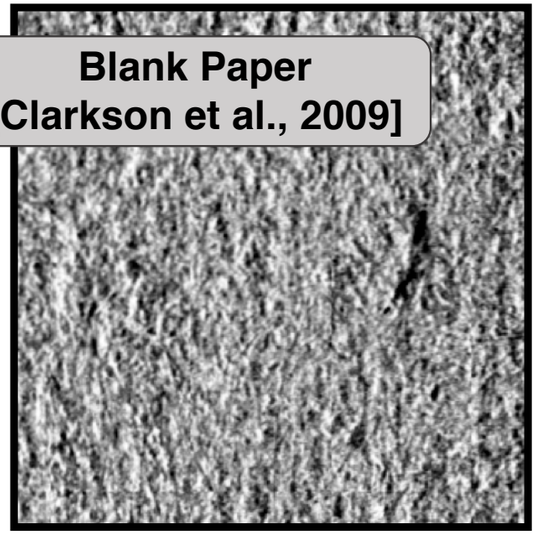


Retina
[Hill, 1978]



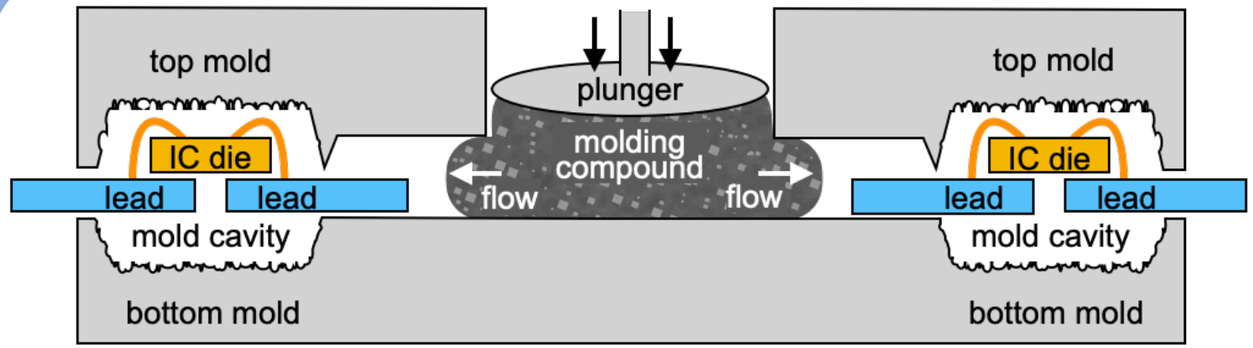
Gait Analysis
[Nixon et al., 1996]

Camera Sensors
[Lukas et al., 2006]

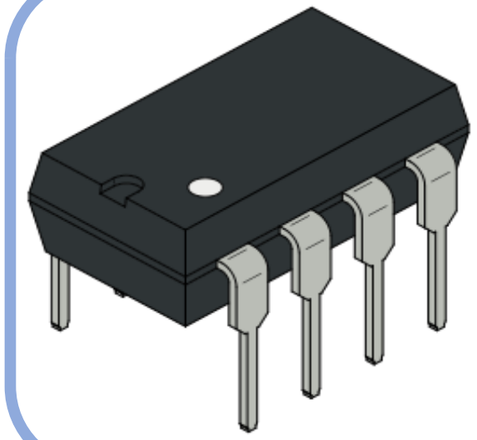


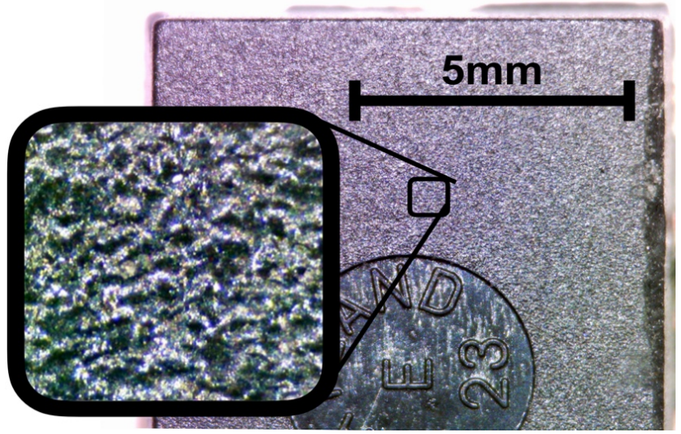
Blank Paper
[Clarkson et al., 2009]

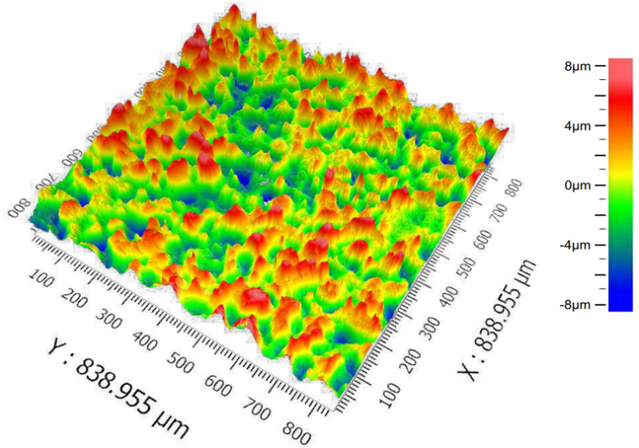
Package Surface Texture

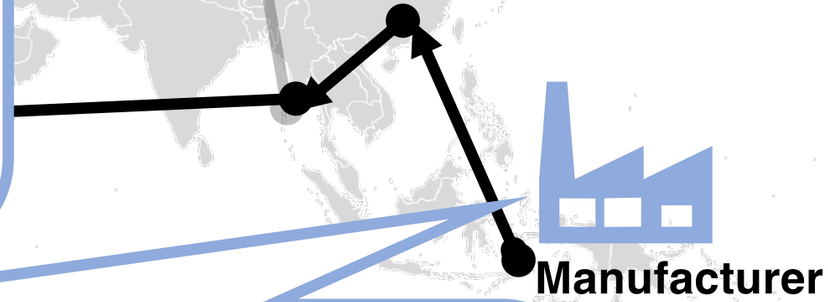


Transfer molding creates plastic package of ICs by forcing liquified molding compound (75% filler) into cavities around wire-bonded ICs and then allowing to cure and harden

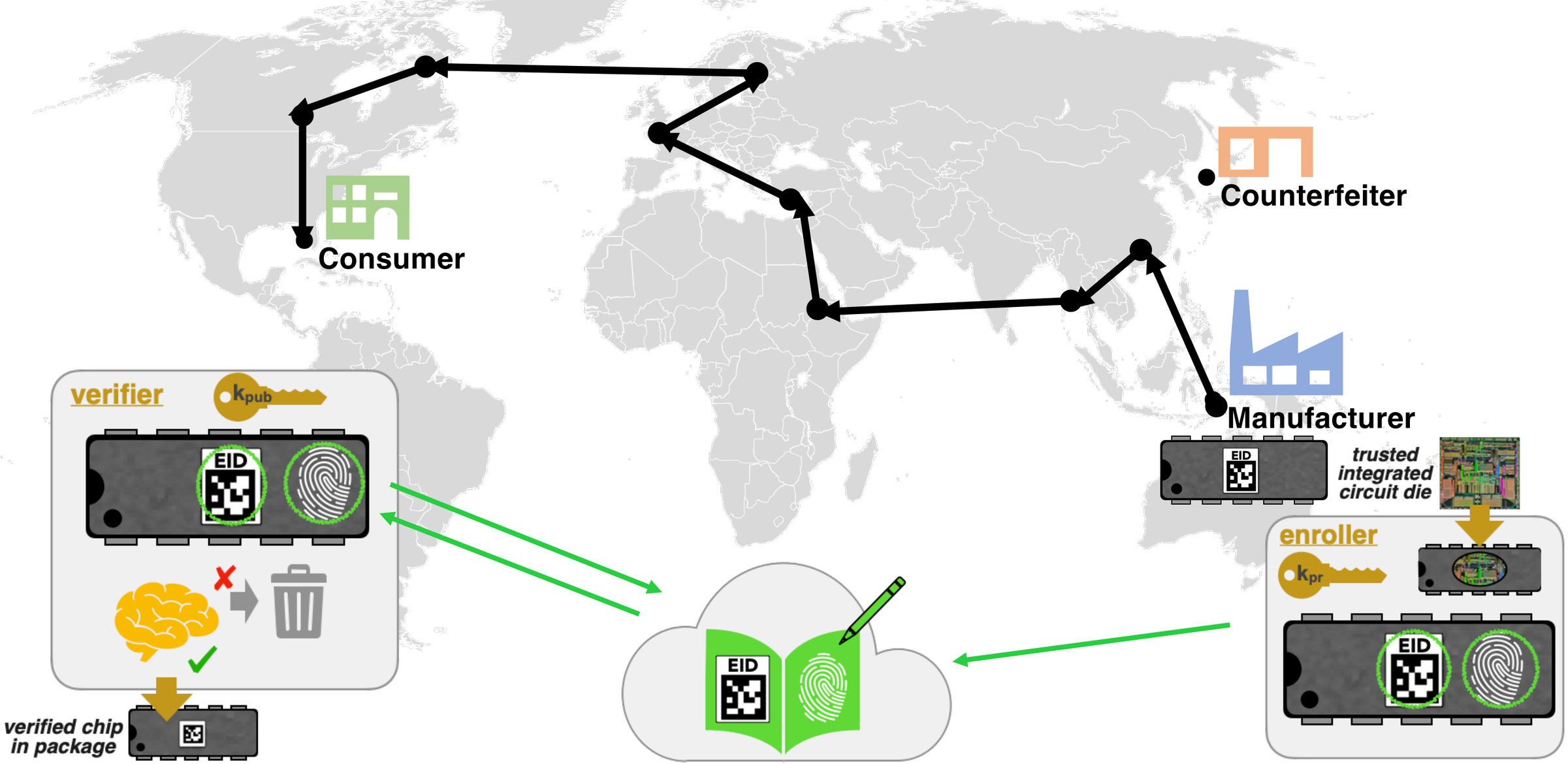




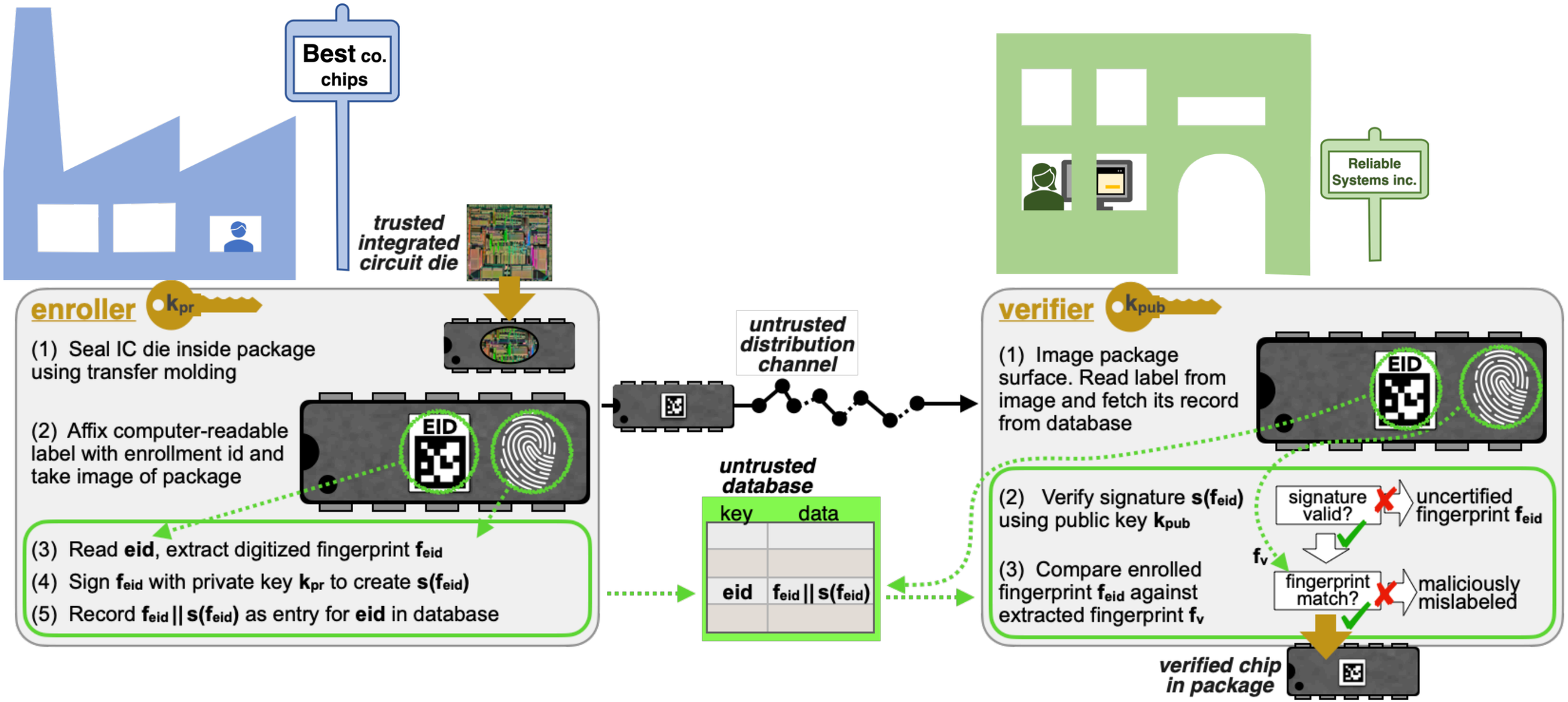




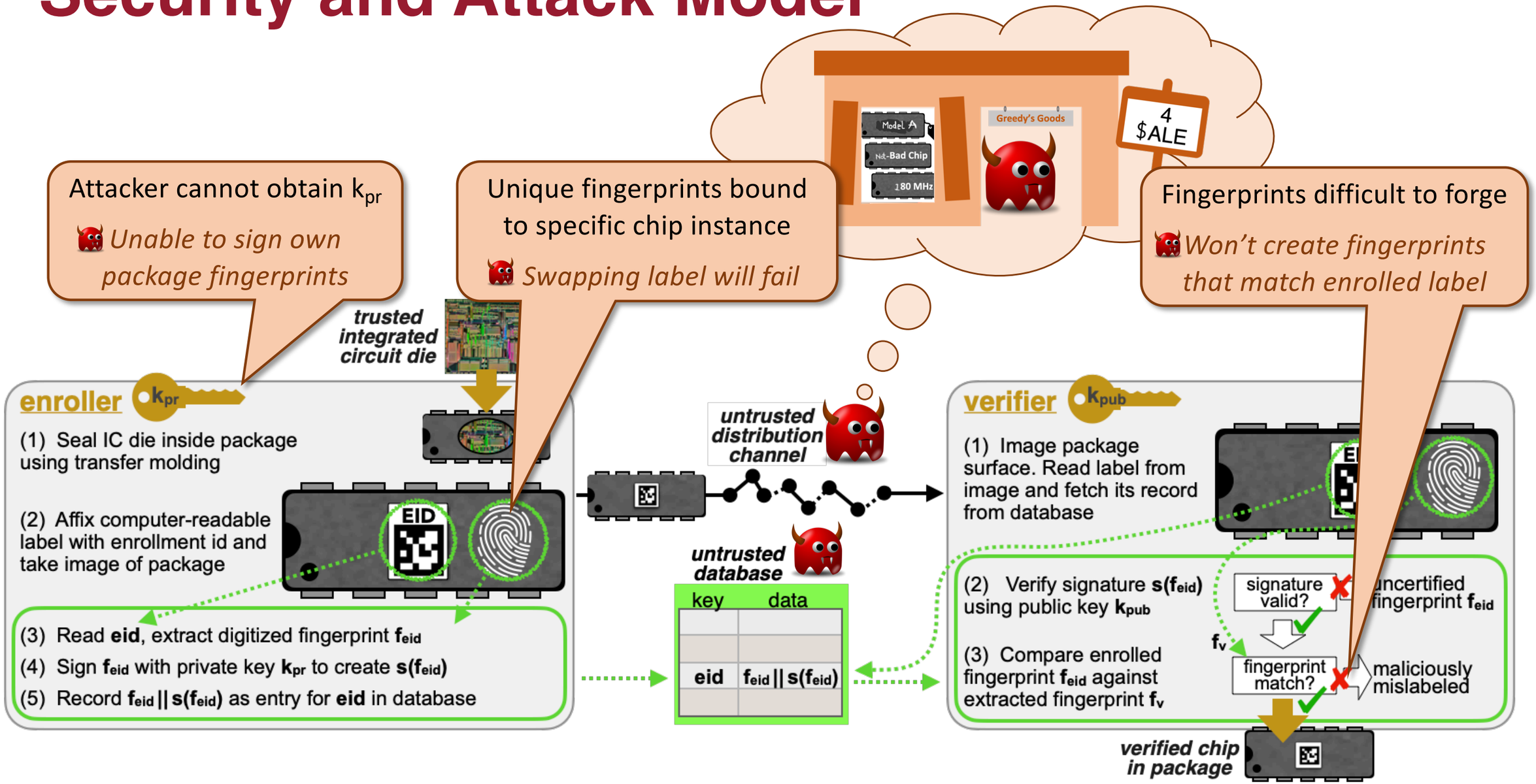
Overview of CounterFoil



Security and Attack Model

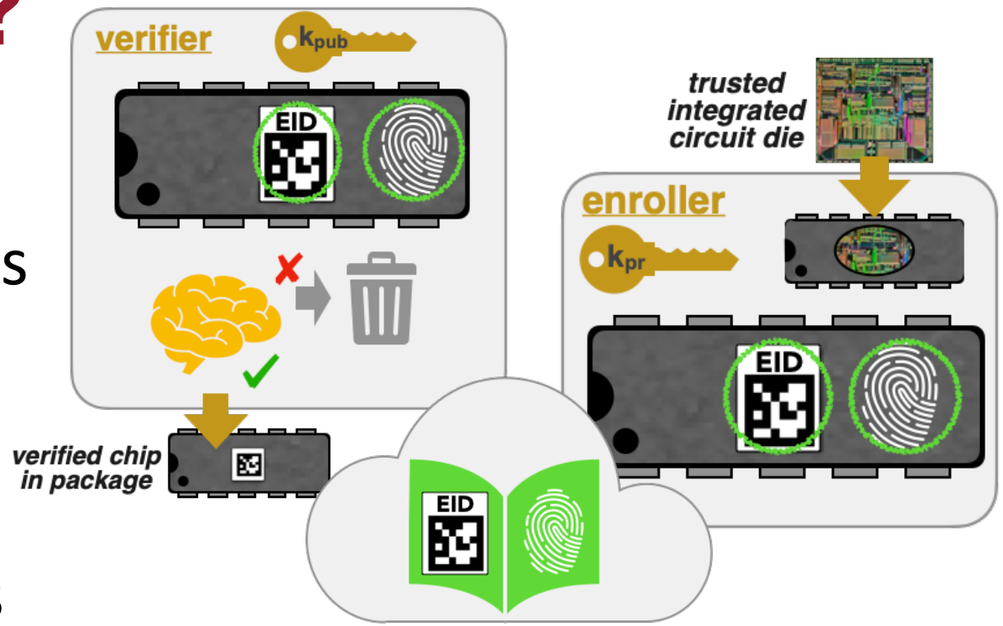


Security and Attack Model

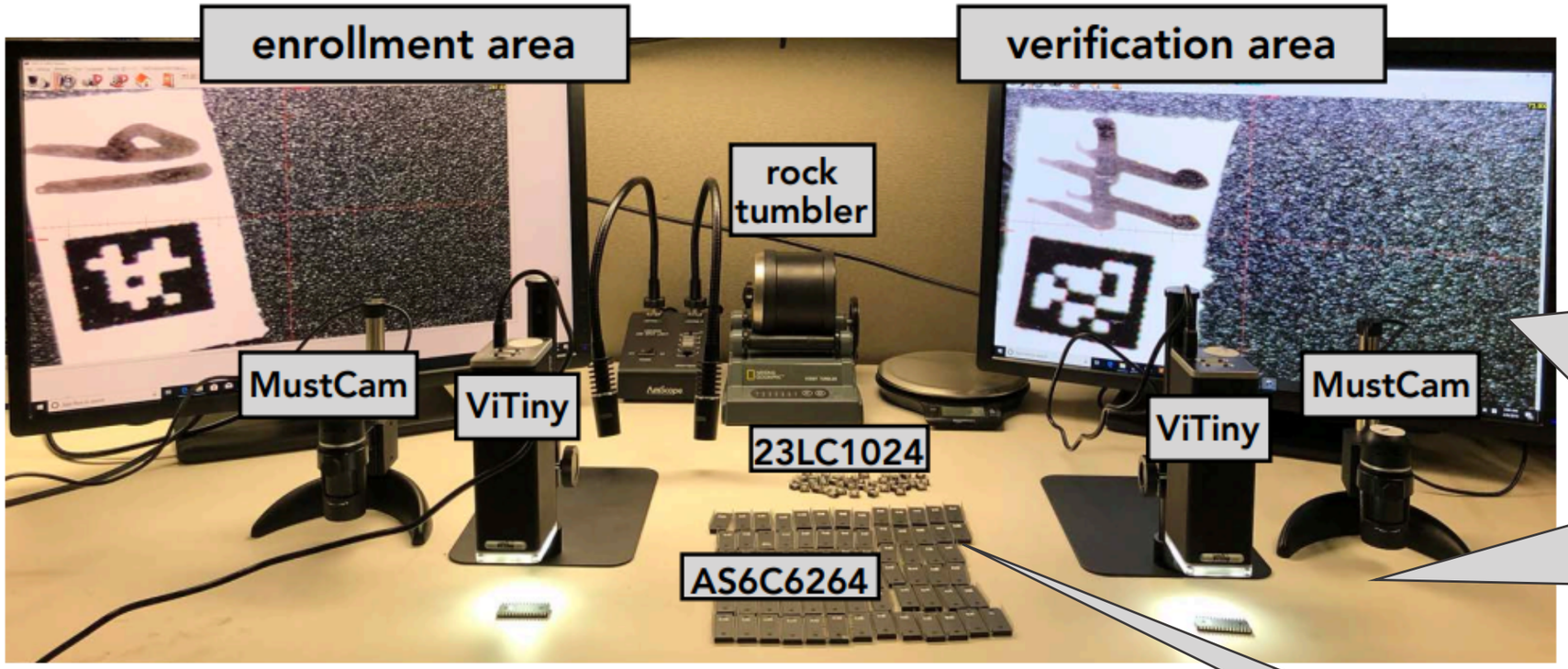


Why CounterFoil?

- Fingerprints extracted from images of plastic IC packages
- Inexpensive cameras
- Verification in 150ms
- Practical scheme that works with existing IC distribution
- Does not require chain of custody

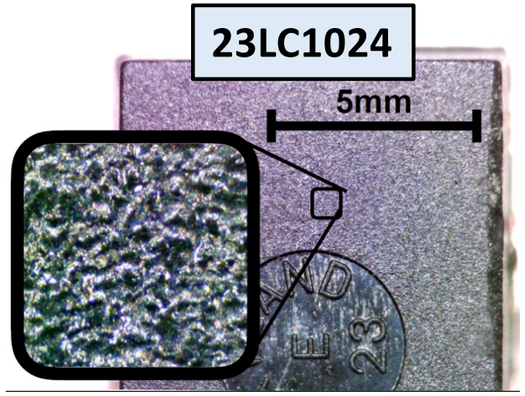


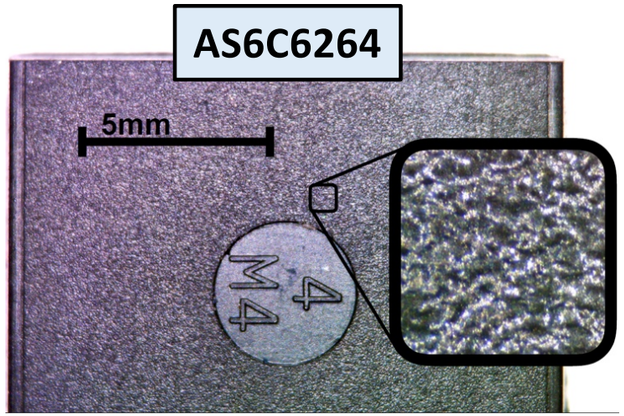
Experimental Setup

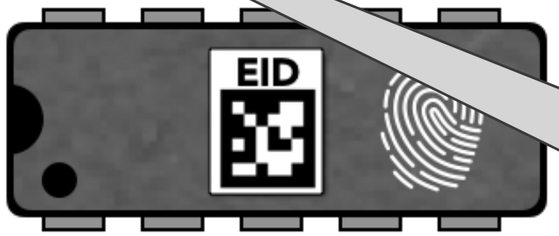


- OpenCV implementation of Computer Vision algorithms
- Crypto++ for processing
- Code/images posted at [1]

- Cameras from two vendors
- Different instances for enrollment and verification





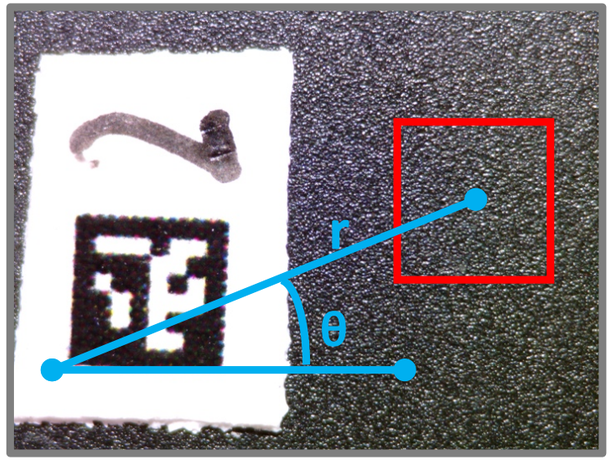


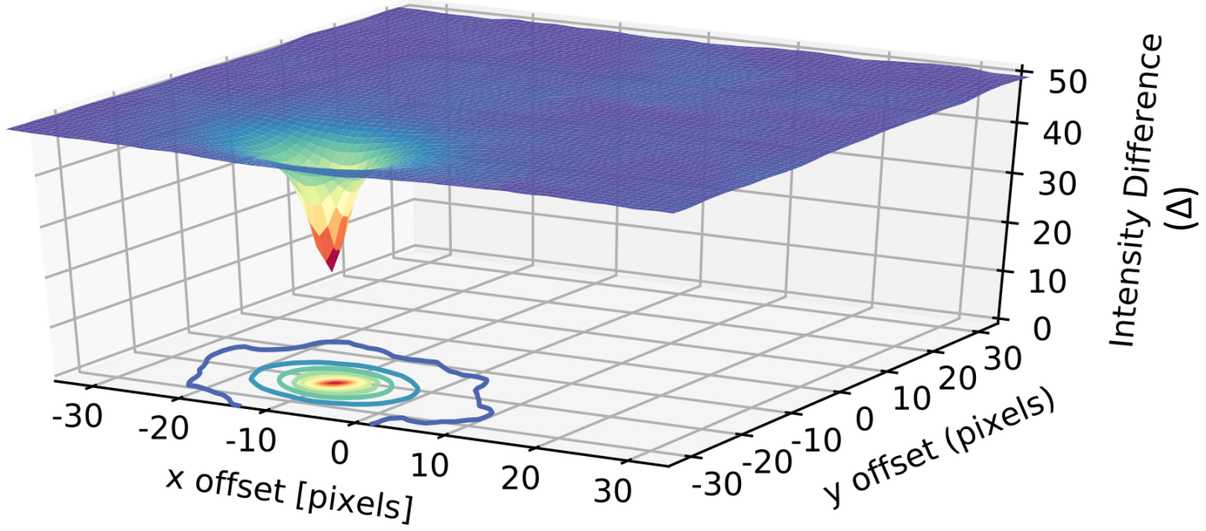
- Two chip models
- Some packaged with the same mold instance

[1] https://github.com/danholcomb/supply-chain-security

Naïve Fingerprinting

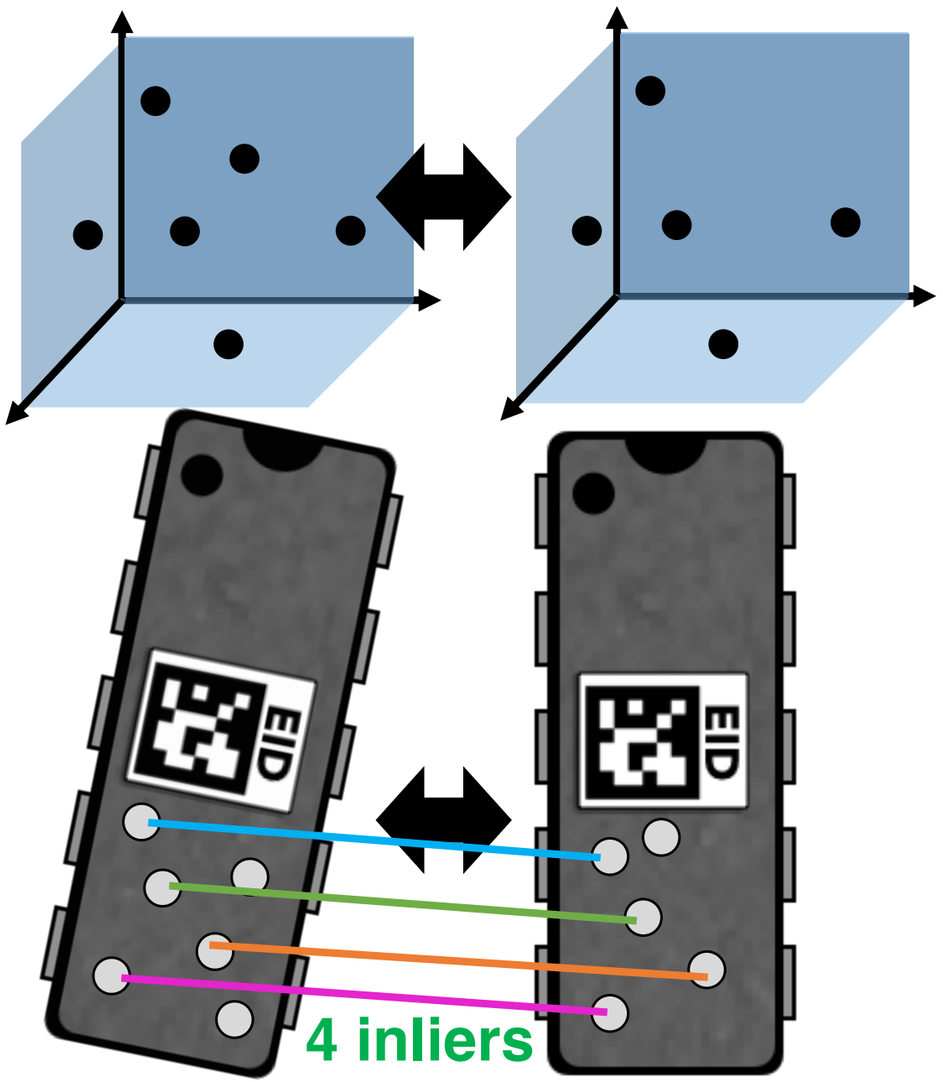
- Use difference in pixel intensity (Δ) to quantify dissimilarity
- Intolerant of misalignment in position, rotation and scale
- Imperfect alignment even with fiducial marks
- Brute-forcing pixel alignment impractically slow



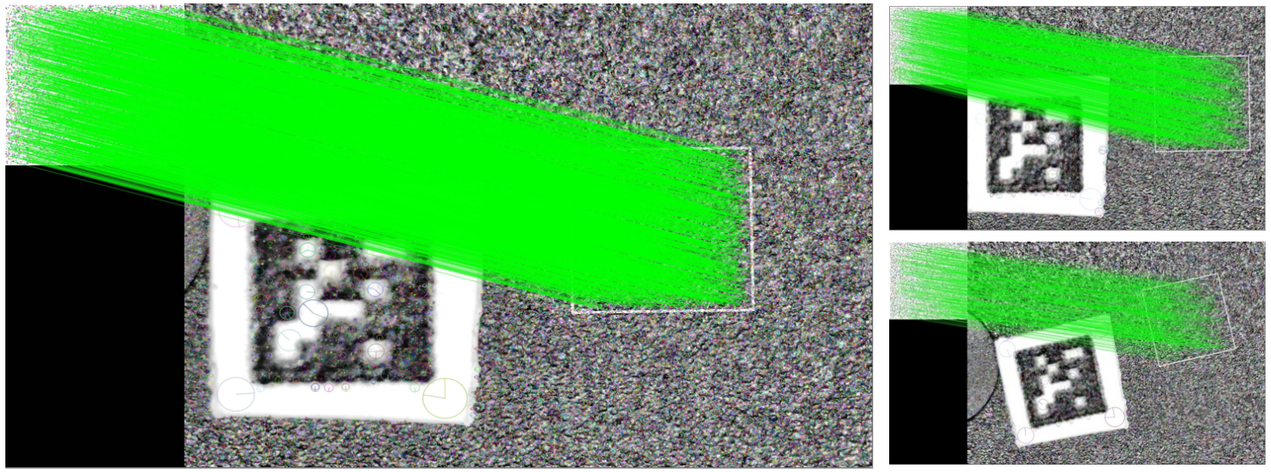


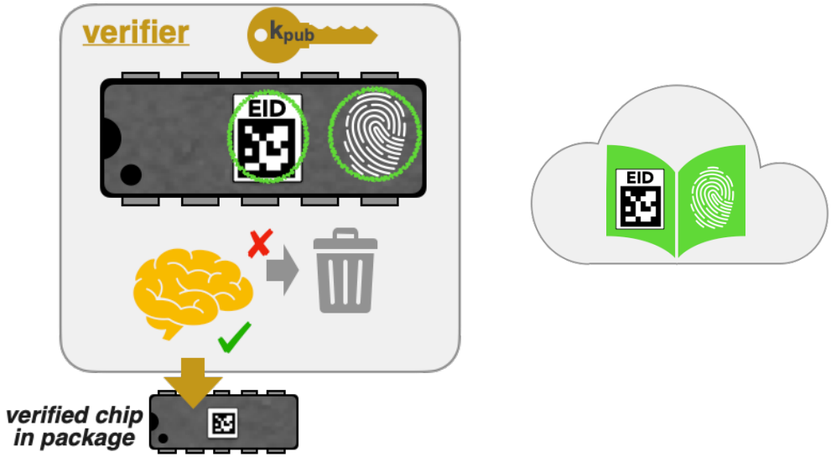
Fingerprinting using Computer Vision

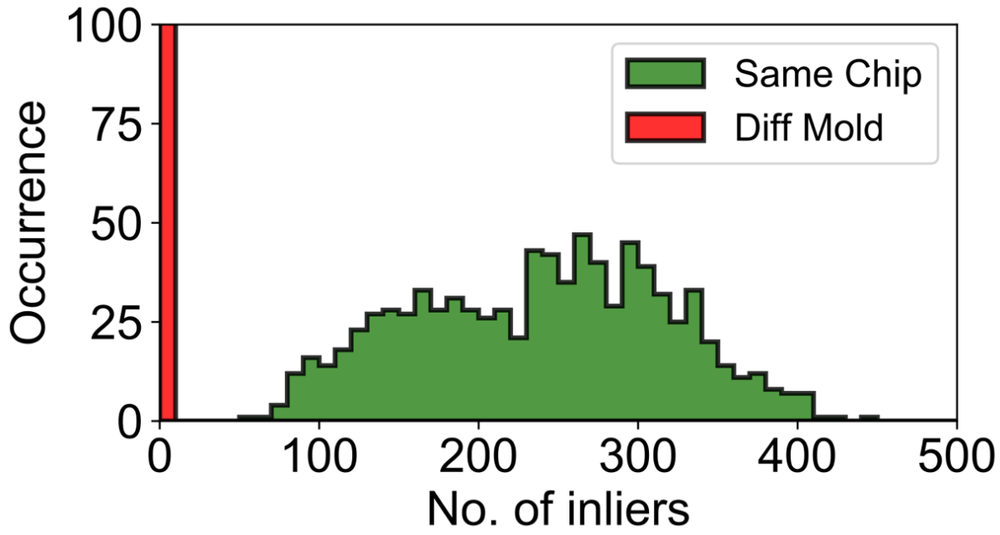
- Identifying features of an image compared rather than each pixel
  - Features used for object detection & matching, motion tracking, stitching panoramic views
- Feature extraction with four prominent algorithms
  - SIFT, SURF, **ORB**, BRISK
- Keypoints: Position and Descriptor
- Matching keypoint is closest in feature space
- Geometry estimation using RANSAC
- **Inlier** only if match is nearest in feature space and fits geometry

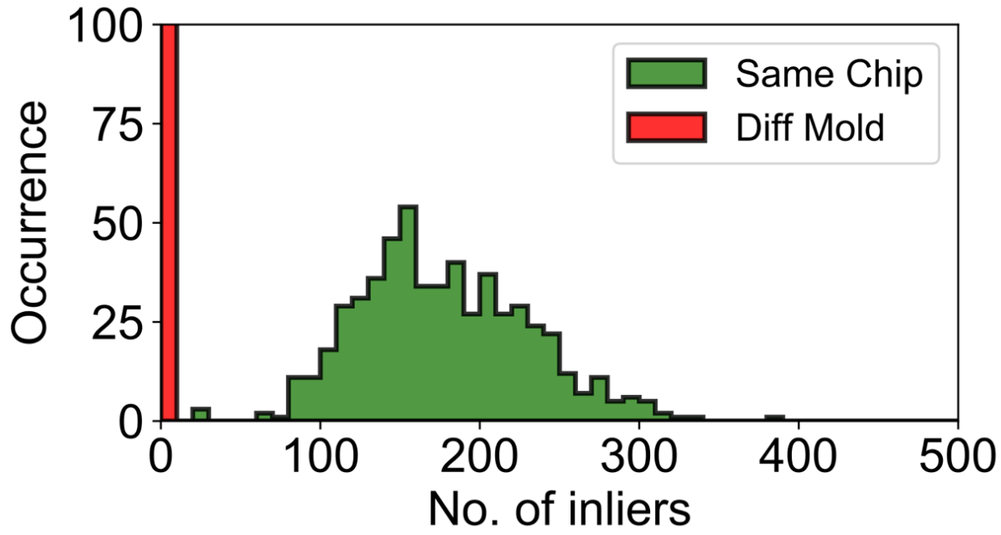


CounterFoil vs Common Attacker



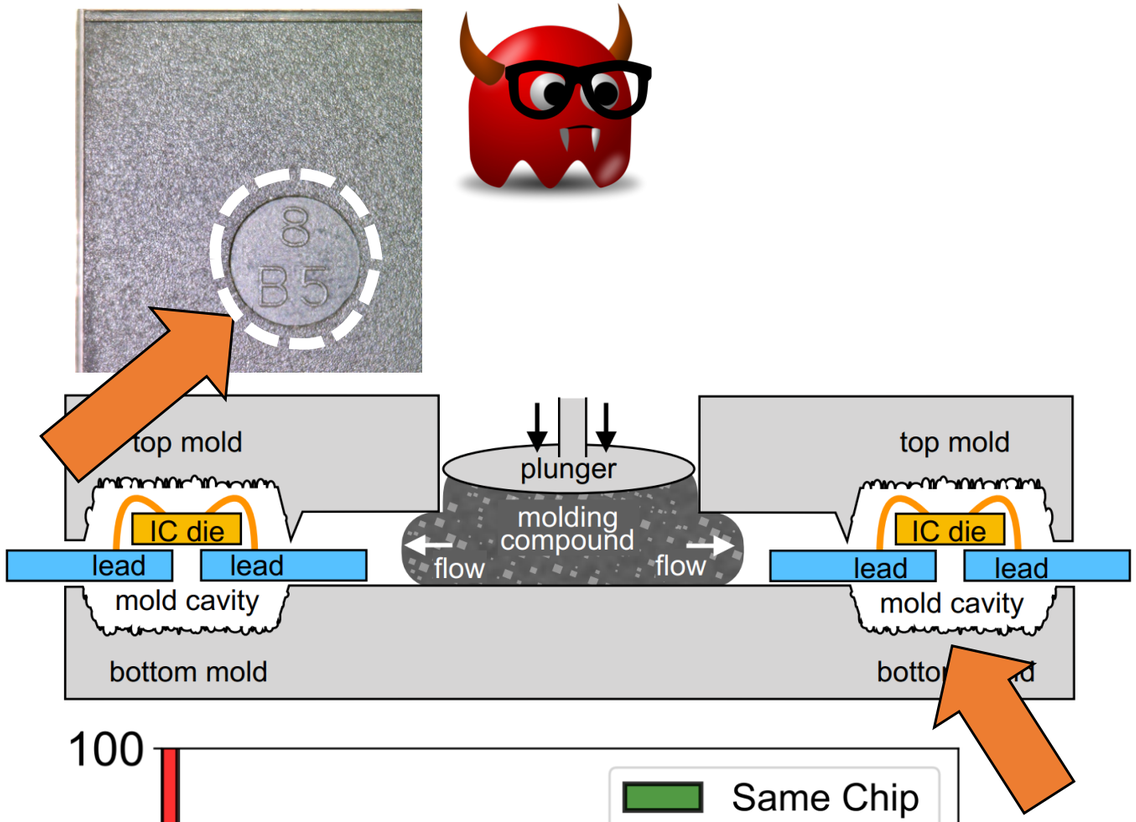


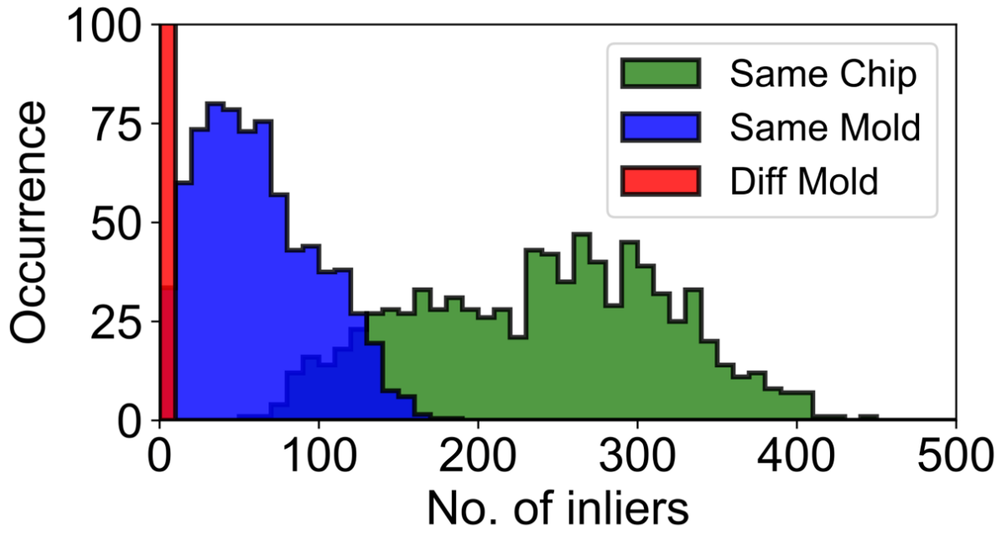


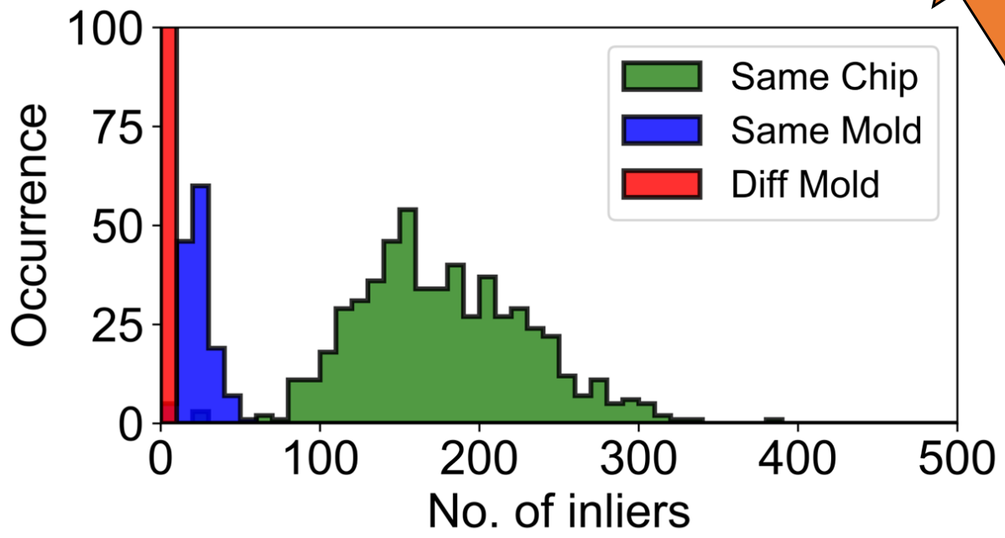


Sophisticated Attacker

- Can a package be forged to match enrolled fingerprint?
  - Consider an attacker that exactly duplicates manufacturer mold
  - Model this attacker using purchased packages produced by same mold instance
  - Revealed by mold marking

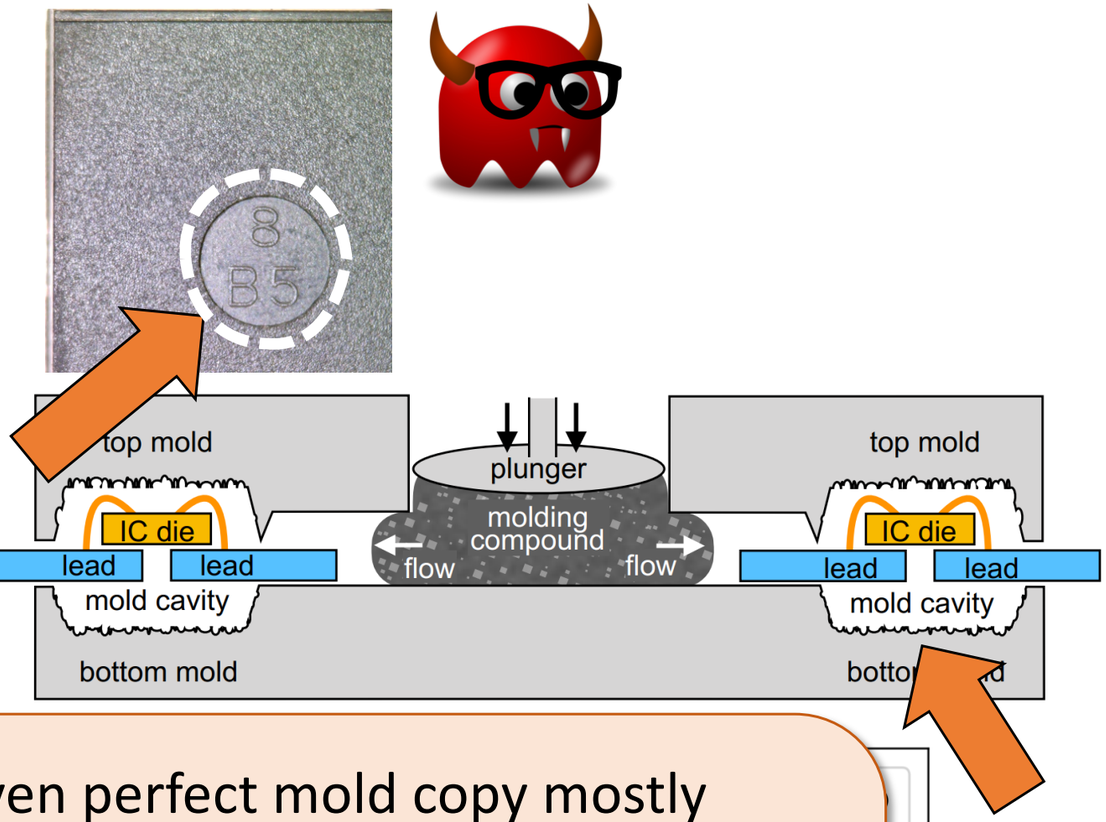


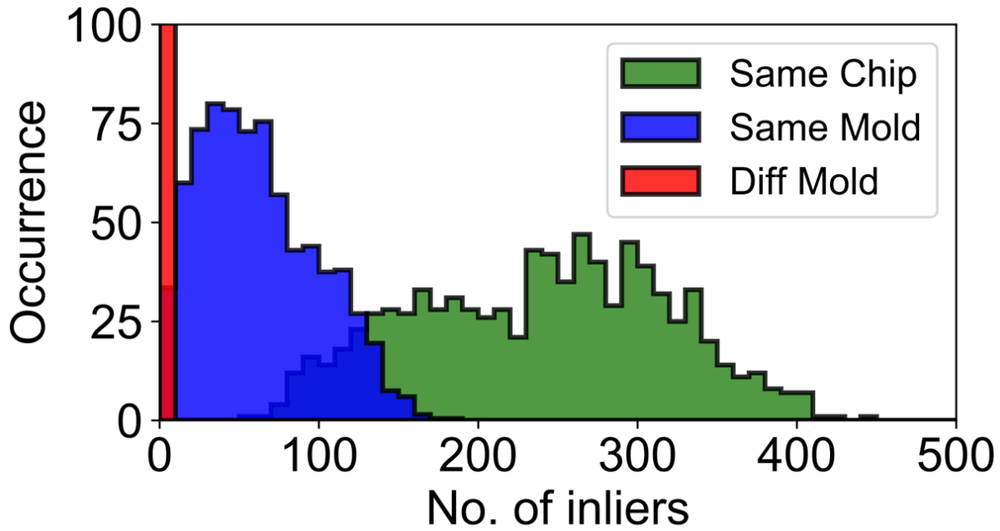




Sophisticated Attacker

- Can a package be forged to match enrolled fingerprint?
  - Consider an attacker that exactly duplicates manufacturer mold
  - Model this attacker using purchased packages produced by same mold instance
  - Revealed by mold marking





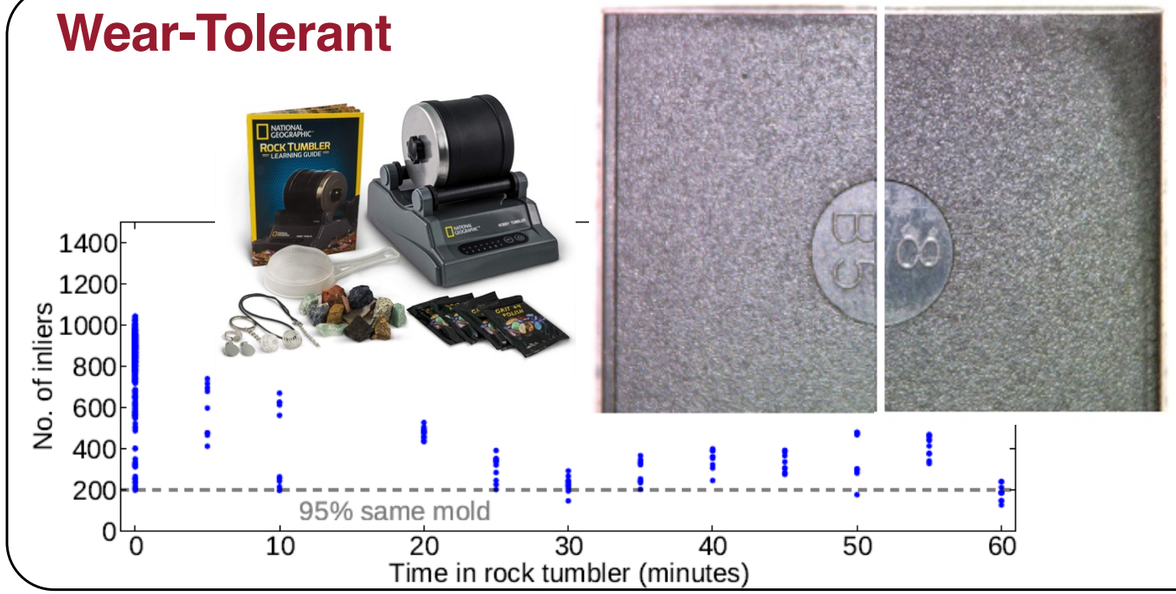
- Even perfect mold copy mostly unsuccessful
  - Filler particles
  - Mold buildup
  - Curing process
- In the worst of 4 datasets, need to allow 16% FP rate for 95% TP rate

Suitability for IC Distribution

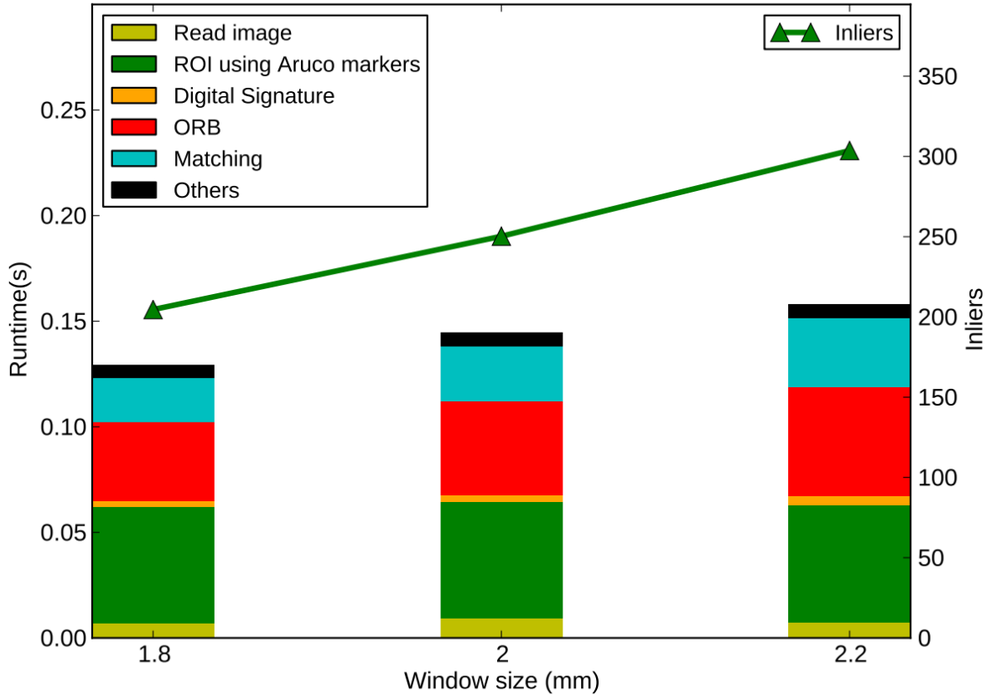
Inexpensive

- Cheap cameras
- Marker costs are negligible
- 1MB storage per enrolled record

Wear-Tolerant

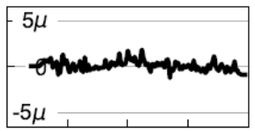
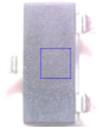
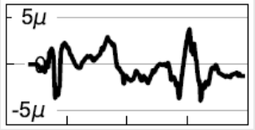
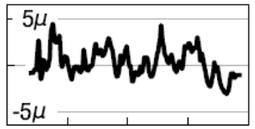
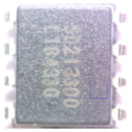
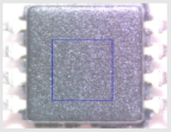
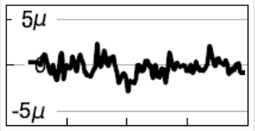
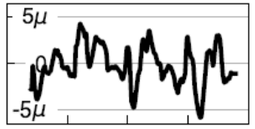
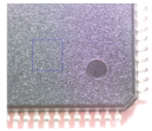
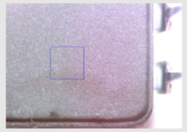
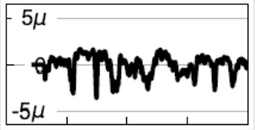
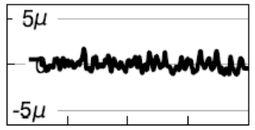
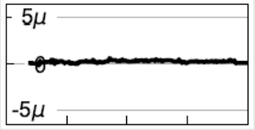
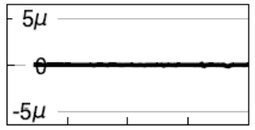
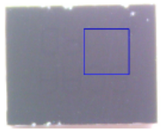
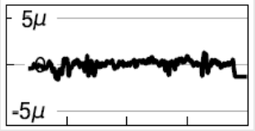


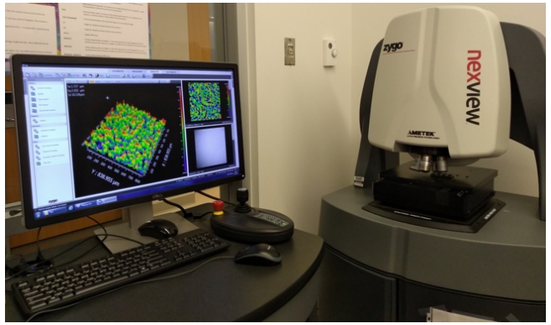
Efficient

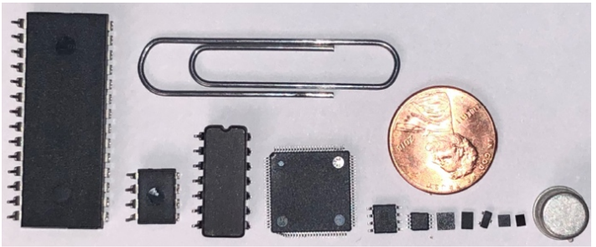


- Authenticate in 150ms on Intel Xeon E5-2690
- Could run real-time on pick-and-place (700ms)

How Broadly Applicable?

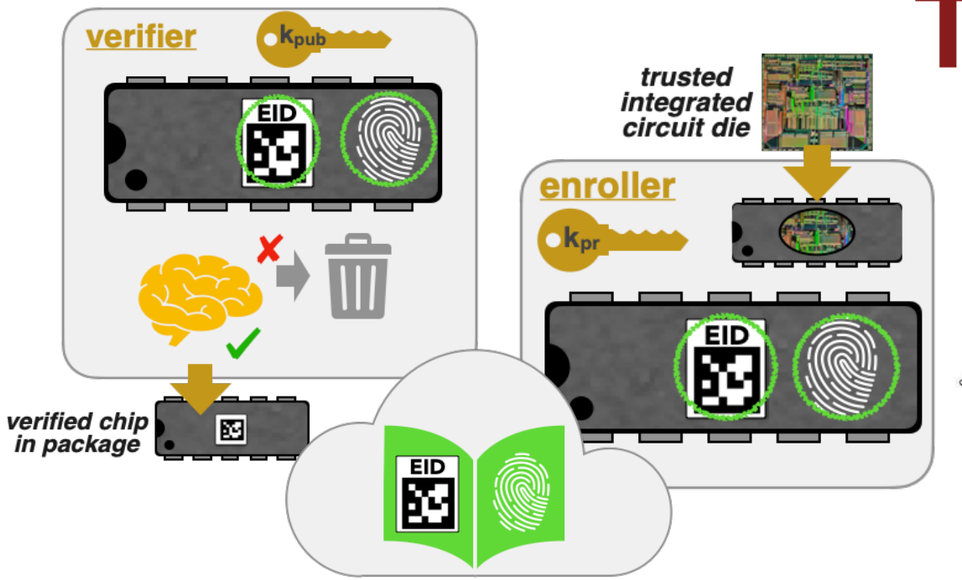
Surface Map	Example Image	Chip Name	Package	Same Chip Inliers μ (σ)	Diff. Chip Inliers μ (σ)	Area (mm^2)	Example Image	Surface Map
		W25Q80EWUXIETR	23-SOT	38.6 (13.2)	3.0 (1.5)	0.454		
		TSV524IQ4T	16-QFN	42.9 (8.4)	4.1 (1.7)	0.315		
		MX25V4006EM1I-13G	8-SOIC	58.8 (10.2)	3.8 (1.5)	0.454		
		24LC32A-I/MS	8-MSOP	344.3 (44.8)	4.0 (1.3)	2		
		CY7C1353G-100AXC	100-TQFP	280.8 (40.1)	4.7 (1.0)	2		
		ADG419TQ	14-CDIP	358.4 (73.2)	3.9 (1.3)	2		
		ADP125ACPZ-R7	8-LFCSP	18.3 (7.2)	3.2 (1.5)	0.315		
		W25Q80EWUXIE TR	8-USON	12.3 (5.9)	2.1 (1.3)	0.201		
		FAN53540UCX	20-WLCSP	3.2 (2.9)	1.8 (1.4)	0.315		
		2N3440	TO-39	0 (0)	0 (0)	2		



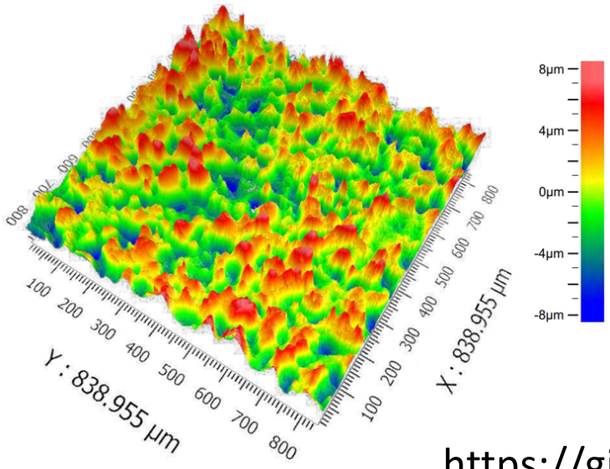


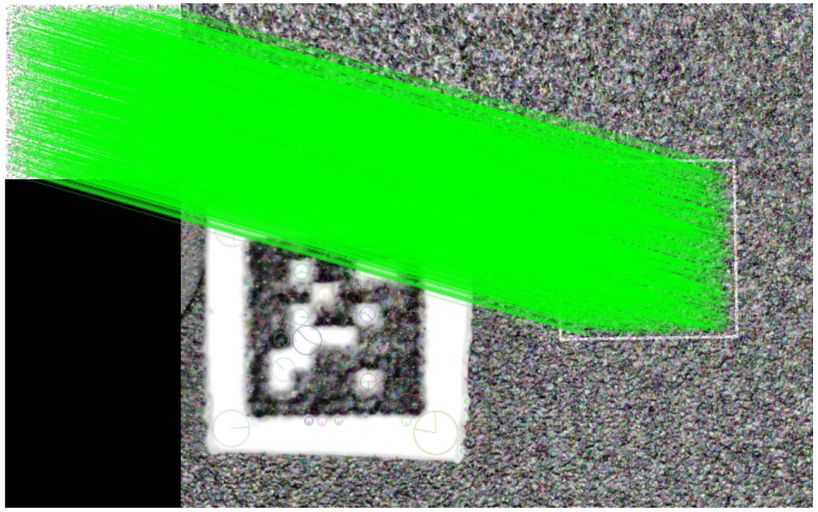
Summary

- Counterfeit ICs threaten critical systems and profits
- CounterFoil verifies IC provenance by using fingerprints from surface texture of plastic packages
- Low cost, high performance and easy to integrate into IC distribution



Thank you!





https://github.com/danholcomb/supply-chain-security