Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
L7: Probability, Encryption

CSU Cybersecurity Center
Computer Science Dep

Loss Ratio

- The loss **ratio is** the ratio of incurred losses and loss adjustment expenses to premiums earned.

$$Loss\ Ratio = \frac{incurred\ losses + loss\ adjustment\ expenses}{premiums\ earned}$$

- *Example:* A company paid $133.6 million in losses and $14 million in loss-adjustment expenses. Premiums earned were $205 million.

$$Loss\ Ratio = \frac{133.6 + 14}{205} = 0.72$$

- The loss ratio is often in the 65 percent to 75 percent range. Thus the insured pool with get back about 65 to75% of the premiums paid. Affordable Care Act (ObamaCare)requires it to be minimum 80% (85% for large groups).

Principles of risk Management and insurance, Rejda, McNamara, 2017

Utility In Insurance

Utility in insurance quantifies the benefit a buyer gains by transferring cyber risk to an insurer, thereby reducing the variability (or uncertainty) of financial losses and increasing the firm's overall expected satisfaction or economic value.

- Risk-averse organizations prefer **more predictable outcomes**, even if the expected value is slightly lower. Cyber insurance provides that.
- Utility function for a risk-averse organization with respect to payment can be of the form (in the example next)

$$u(w) = w^{0.5}$$

- The goal is to **maximize expected utility**, not just expected profit.

Utility Example: Football Player

Player's utility function is $u(w) = w^{0.5}$
where w is the earning from the game.

- Player earns $1 million if healthy.
- There is a 10% probability the player is injured and earns $0

E(u) = Prob(healthy).u(if healthy)+(1- Prob(healthy)).u(if injured)

$= 0.9 \times (1{,}000{,}000)^{0.5} + 0.1 \times (0^{0.5}) = 900$

Actuarially fair insurance premium

=prob(loss) x size of loss = 0.1 x 1,000,000 = $100,000

Earnings with insurance (premium paid is $ 100,000)

- Healthy: $1 mill. -100,000 = $900,000
- Injured: $0 - 100,000 + $1 mill. (from insurance)
  = $900,000 same! (as expected)

But consider utility

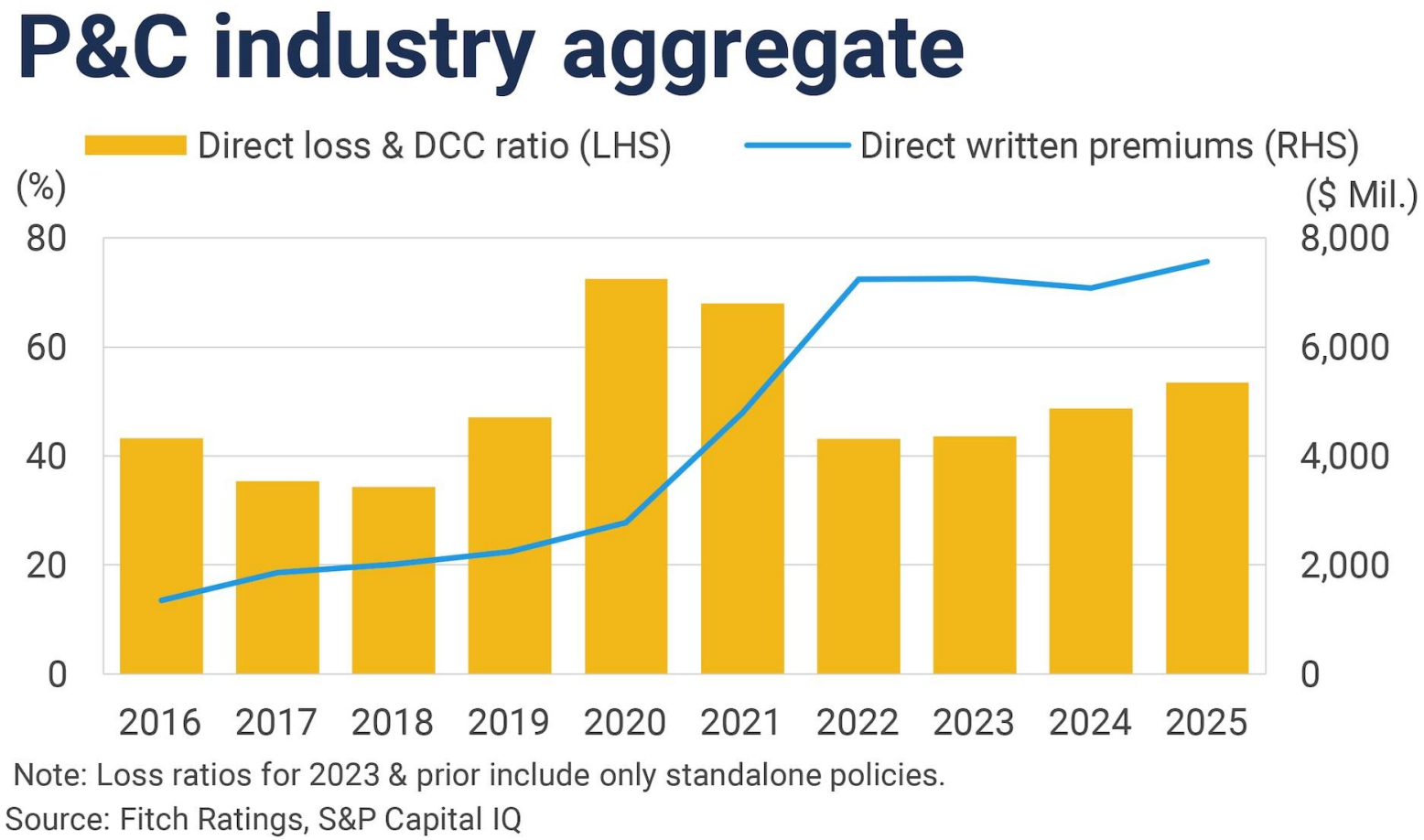
E(utility with insurance)

$= 0.9 \times (900{,}000^{0.5}) + 0.1 \times (900{,}000^{0.5})$

$= 948.7$

which is better than E(utility without insurance) of 900.

Loss ratio for U.S. standalone cyber policies – 2016 to 2025



https://www.theinsurer.com/cyber-risk/news/fitch-us-cyber-insurance-market-swung-to-7-written-premium-growth-in-2025-2026-06-03/

Colorado State University

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
Probabilistic Perspective

CSU Cybersecurity Center
Computer Science Dep

Conditional Probability

- Conditional probability

$$P\{A \mid B\} = \frac{P\{A \cap B\}}{P\{B\}} for P\{B\} > 0$$

P{A|B} is the probability of A, given we know B has happened.

- If A and B are independent, P{A|B}= P{A}. Then

$$P\{A \cap B\} = P\{A\}P\{B\}$$

- Example: A toss of a coin is independent of the outcome of the previous toss.

Conditional Probability

- If A can be divided into disjoint A_i, i=1,..,n, then

$$P\{B\} = \sum_i P\{B \mid A_i\} P\{A_i\}.$$

- Example: A chip is made by two factories A and B. One percent of chips from A and 0.5% from B are found defective. A produces 90% of the chips. What is the probability a randomly encountered chip will be defective?
- P{a chip is defective} = (1/100)x0.9 + (0.5/100)x0.1

  =0.0095 i.e., 0.95%

Bayes' Rule 1763

- Conditional probability

$$P\{A \mid B\} = \frac{P\{A \bigcap B\}}{P\{B\}} for P\{B\} > 0$$

P{A|B} is the probability of A, given we know B has happened.

- Bayes' Rule

$$P\{A \mid B\} = \frac{P\{B \mid A\}P\{A\}}{P\{B\}} for\, P\{B\} > 0$$

$$P\{A|B\} = \frac{P\{B|A\}P\{A\}}{P\{B|A\}P\{A\}+P\{B|\sim A\}P\{\sim A\}}$$

Bayes' Rule Example

P{A|B} is the probability of A, given we know B has happened.

- Bayes' Rule

$$P\{A \mid B\} = \frac{P\{B \mid A\}P\{A\}}{P\{B\}} \; for \; P\{B\} > 0$$

- Example: A drug test produces 99% true positive and 98% true negative results. 0.5% are drug users. If a person tests positive, what is the probability he is a drug user?

$$P\{DU \mid P\} = \frac{P\{P \mid DU\}P\{DU\}}{P\{P \mid DU\}P\{DU\} + P\{P \mid nDU)P\{nDU\}}$$

$$= \quad ?$$

Bayes' Rule

Example: A drug test produces 99% true positive and 98% true negative results. 0.5% are drug users. If a person tests positive, what is the probability he is a drug user?

$$P\{DU|P\} = \frac{P\{P|DU\}P\{DU\}}{P\{P|DU\}P\{DU\}+P\{P|nDU\}P\{nDU\}}$$

$$= \frac{0.99\times0.005}{0.99\times0.005+0.02\times0.995} = 0.1991$$

= 19.91%%

Person is a drug user and test result is positive: True Positive
P{P|DU} = 0.99 (99%)

Person is not drug user and test result is negative: True Negative
P{N|nDU} = 0.98 (98%)

P{P|nDU} = 1-0.98 = 0.02

Frequentist statistics:

- probability as the limit of the relative frequency of an event after many trials

Baysian statistics:

- based on the Bayesian interpretation of probability - expresses a degree of belief in an event. The degree of belief may be based on the results of previous experiments, or past personal experiences.

Bayes' Rule: Posterior Probability

- Implications of Bayes' rule:

$$P\{A \mid B\} = \frac{P\{B \mid A\}P\{A\}}{P\{B\}} \; for \; P\{B\} > 0$$

- P{A} represents prior probability, when we did not know about B.
- P{A|B} represents posterior probability, after we know B.
- Probability changes if we know more!

- Average age of student = 23 years
- Average age of student| a graduate student = 33 years

Binary Classification Problem

Binary classification problem

- **There are no perfect tests for diseases.**
- **There is no intrusion detection algorithm that is perfect.**

	Disease +	Disease -
Test +ve	TP	FP
Test –ve	FN	TN

We may want to know

- If the person has the disease, what is the prob test is positive?
- If the person does not have the disease, what is the prob test is indeed negative?
- If the result is positive, what is the prob it is true?
- If an intrusion detection algorithm claims it has detected an intrusion, what is the probability there is actually no intrusion?

Collect available past data to estimate these.

Confusion Matrix

	Disease +	Disease -
Test +ve	TP	FP
Test –ve	FN	TN

- Sensitivity = TP/(TP+FN) also TPR true pos rate
  - If the person has the disease, what is the prob test is positive?
- Specificity = TN/(FP+TN) also TNR true neg rate
  - If the person does not have the disease, what is the prob test is indeed negative?
- Precision = TP/(TP+FP) PPV positive predictive value
  - If the result is positive, what is the prob it is true?
  - Ex: TP= 580, FP = 21, FN = 308, TN = 105

    Precision = 580/(580+21) = 0.965
- Several other measures used. For example
  - F1 score = 2TP/(2TP + FP + FN)

RT-PCR s	Disease +	Disease -
Test +ve	580	21
Test –ve	308	105

Example: Intrusion Detection

If an ID scheme is more sensitive, it will increase false positive rates.

- Ex Car alarm

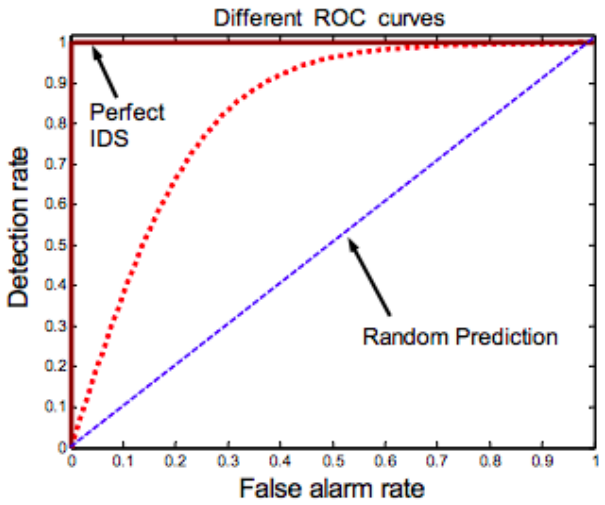


Figure 2-5. ROC Curves for different intrusion detection techniques

- Detection rate (True Positive rate, sensitivity) vs False Positive Rate. We want detection rates to be higher for the same false positive rate.
- Area under the ROC curve is a good measure of the ID scheme.

"ROC" **receiver operating characteristic** we don't care why.

Intrusion Detection A Survey, Lazarevic, Kumar, Srivastava, 2008

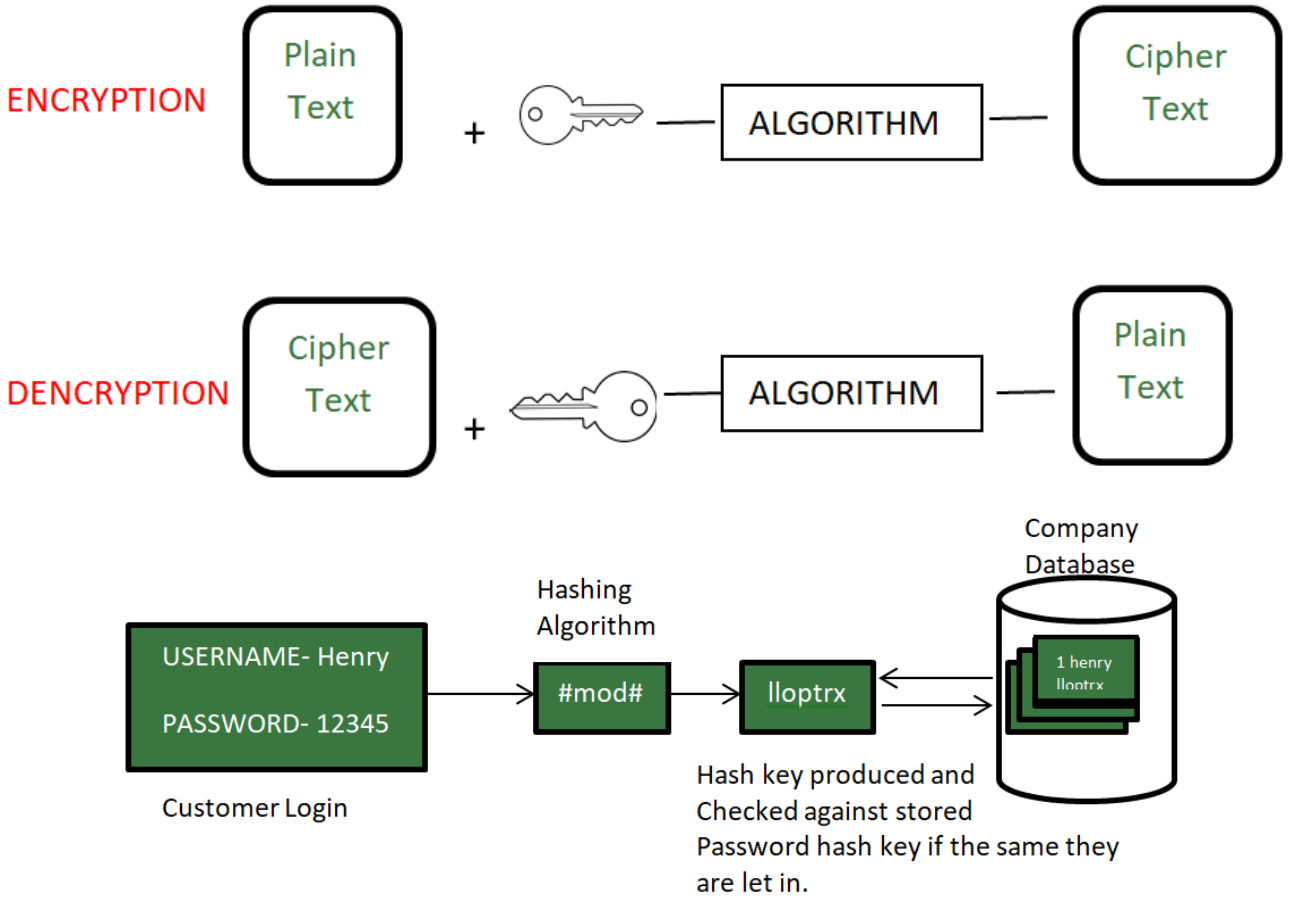
Quick Project Presentations

- Presentations Sept 15, 17 coming week
  - Schedule will be on Canvas discussions
- 12-15 min presentations for each person, 12 slides
  - Need time for discussions
  - When two persons have the same topic, they must collaborate, to minimize overlap. The presentations will be scheduled one after the other.
  - Post slides/abstract 24 hours in advance Canvas Discussions in Quick Research Abstract and presentation forum
  - Everyone should preview upcoming presentations
  - Online section: Submit abstract, presentation and a link to your video by Tuesday 5 PM.
    - Slides: Video: same limits
- On-campus: 5-10 minutes discussion for each presentation
- Everyone must view all presentations, comment/questions on at least half of the presentations
- Provide feedback using the Peer Review form due 9/19 Sat. Also do a detailed review of two assigned reports.

Peer Review form

- Will be available soon in Canvas. Due Sept 19, Sat.
- Evaluate each category using 10-point scale.
  - 10: top 25%, 9: next 25%, 8: next 25%, 7: bottom 25%.
  - 25% is about 7 students.
  - Overall score should be average of the other 4 scores.

Symmetric Encryption vs Hashing

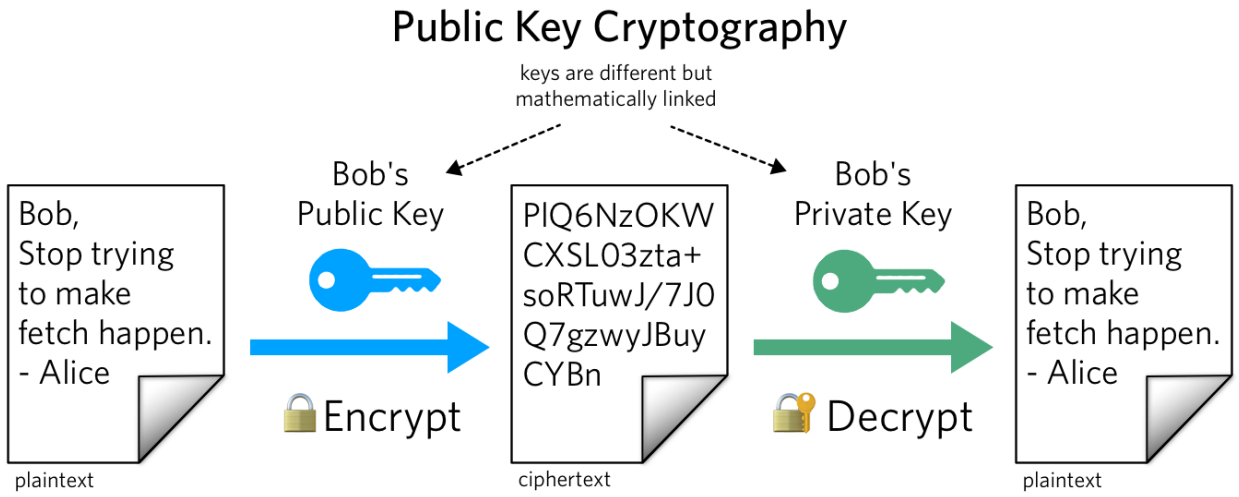


- Impossible to reconstruct password from hash but ..

What is Public Key Cryptography?

In public-key cryptography, also known as asymmetric cryptography, each entity has two keys:

- Public Key — to be shared
- Private Key — to be kept secret
- These keys are generated at the same time using an algorithm and are mathematically linked. When using the RSA algorithm, the keys are used together in one of the following ways:



https://www.twilio.com/en-us/blog/developers/tutorials/building-blocks/what-is-public-key-cryptography#What-is-Public-Key-Cryptography

Using the Public and the Private key

When using the RSA algorithm, the keys are used together in one of the following ways:

1. Encrypting with a public key

   Use case: sending messages only the intended recipient can read.

   Bob encrypts a plaintext message with Alice's public key, then Alice decrypts the ciphertext message with her private key. Since Alice is the only one with access to the private key, the encrypted message cannot be read by anyone besides Alice.

2. Signing with your private key

   Use case: verifying that you're the one who sent a message.

   Alice encrypts a plaintext message with her private key, then sends the ciphertext to Bob. Bob decrypts the ciphertext with Alice's public key. Since the public key can only be used to decrypt messages signed with Alice's private key, we can trust that Alice was the author of the original message.

- These methods can also be combined to both encrypt and sign a message with two different key pairs.

Use Cases of Public-Key Cryptography

- SSH
- TLS (HTTPS, formerly SSL)
- Bitcoin
- PGP and GPG
- Authentication
- Public Key Infrastructure (PKI) used for things like SHAKEN/STIR

Public Key Cryptography Algorithms

- RSA (Rivest–Shamir–Adleman): The current NIST recommendations for RSA is to use at least 2048 bits for your key
- Diffie–Hellman: The Diffie–Hellman approach involves two people building a shared secret key together.
- Elliptic-Curve Cryptography (ECC): smaller key sizes. Using in Bitcoin.

RISKS MITIGATED / CREATED BY

Password Managers and Passkeys

A quantitative review of adoption, credential-vault risk,
and FIDO2/WebAuthn phishing resistance

Vincent Ogbonna

CS559 Quantitative Security

SECTION 1

Current Status of the Technology

PM

Password Managers

Generate, store, and autofill unique high-entropy credentials in an **encrypted vault** protected by a single master password.

Examples:
1Password, Bitwarden, Dashlane, Google Password Manager, Apple Keychain

---

Residual risk: a single master password concentrates access to every stored credential.

PK

Passkeys (FIDO2 / WebAuthn)

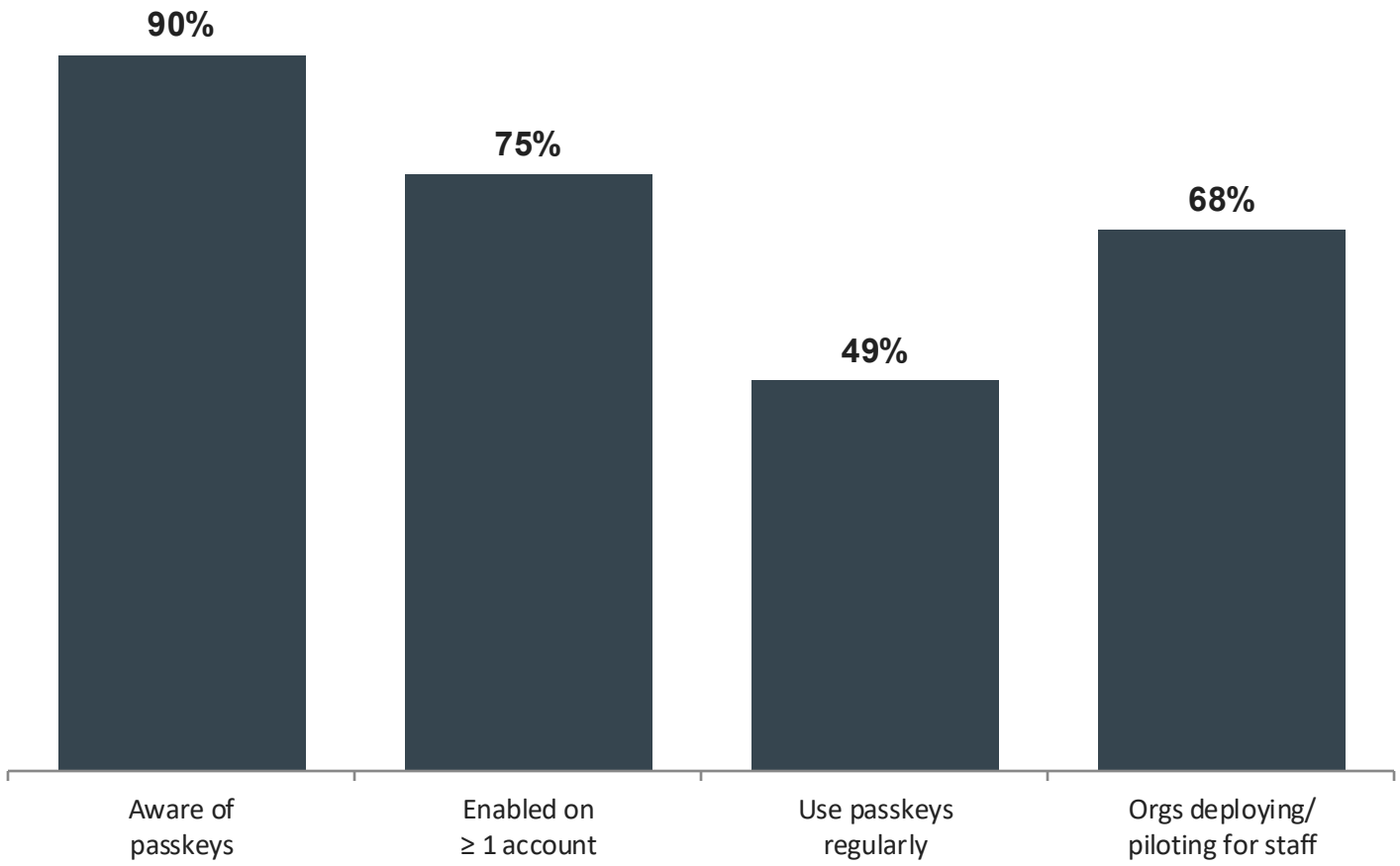
A public/private key pair is generated per website. The **private key never leaves** the user's device or synced keychain; login completes via local biometric or PIN unlock.

~5 billion passkeys in active use worldwide (2026)

The two technologies are converging: mainstream password managers (1Password, Dashlane, Bitwarden, Google, Apple, Microsoft) now generate, sync, and autofill passkeys alongside passwords.

Source: FIDO Alliance, State of Passkeys 2026 [1]

Global Passkey Adoption, 2026



40 pt

gap between awareness (90%) and habitual use (49%)

Survey basis:

11,000 consumers and 1,400 enterprise decision-makers across 10 countries

Awareness has clearly outpaced habitual use — the adoption curve still has room to run.

Source: FIDO Alliance, State of Passkeys 2026 [1]

Recent Developments (2022 – 2026)

2022

LastPass two-stage breach; encrypted vault backups for ~25–30M users exfiltrated

2022–23

FIDO Alliance, Google, Apple & Microsoft commit to a common, syncable passkey standard

2023–25

Google (Oct. 2023) and Microsoft (May 2025) default to passkeys; ~120% growth in usage

2024–25

NIST finalizes SP 800-63-4 / 800-63B-4, elevating FIDO passkeys to the AAL2/AAL3 baseline

2025

$24.5M LastPass class-action settlement; UK ICO issues a monetary penalty

2026

USENIX Security audits 872 passkey sites; ~51% of 103 tested had a high-severity flaw

Sources: report Sec. 2, refs. [2], [3], [4], [5], [6]

SECTION 3

Current Products and Mature Technologies

Category	Examples	Passkey Support
Password managers	1Password, Bitwarden, Dashlane, NordPass	Yes — store & sync passkeys
Platform keychains	Apple Keychain/Passwords, Google Password Manager, Windows Hello	Native, default on billions of devices
Hardware keys	YubiKey, Titan Security Key	Device-bound FIDO2 authenticator
Standards bodies	FIDO2 / CTAP2, W3C WebAuthn	Underlying interoperable protocol

Takeaway: Passkey support is now built into every major layer of the credential stack — vault software, OS keychains, and dedicated hardware — all interoperating over the same FIDO2/CTAP2 and WebAuthn standards.

Risk Created: Offline Vault Cracking

$$T \approx 2^{H} / (2 \cdot R)$$

H = master-password entropy (bits) *R = guesses attempted per second*

Expected time to exhaustively search the key space, once an attacker holds the encrypted vault.

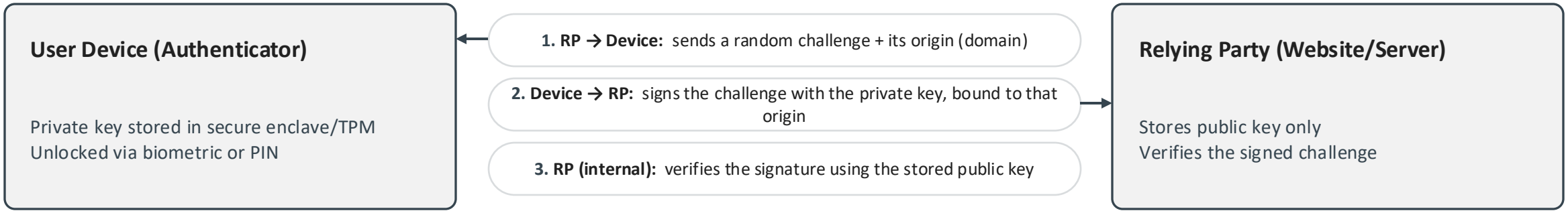
LastPass key-derivation function used as few as **1–100 iterations** on early accounts, vs. the **600,000** iterations recommended today — a 3–4 order-of-magnitude difference in effective R for the same hardware budget.

Reported Impact — 2022 LastPass Breach	
Customer accounts affected	~25–30 million
Crypto theft linked by Sept. 2023 (Krebs)	$35M+ / 150+ victims
Cumulative crypto theft, 2025–26	$150M–$200M+
Class-action settlement (2025)	$24.5 million

Sources: Krebs on Security [3]; U.S. Secret Service/FBI seizure filing [2, 7]

SECTION 4.3

Risk Mitigated: The Passkey Authentication Ceremony



Origin-bound cryptographic signature ⇒ credentials cannot be replayed or phished on a look-alike domain (unlike a typed password).

Because the private key never leaves the device and is bound to the exact origin it was created for, **the credential itself cannot be phished, reused across sites, or made useful if stolen** — a server-side breach exposes only public keys, which are worthless to an attacker alone. This directly closes off credential stuffing and classic phishing, which together drive most account-takeover incidents.

Basis: FIDO2 / W3C WebAuthn specification (report Fig. 2)

Residual Risk: The 2026 USENIX Security Audit

872

passkey-enabled sites tracked

103

sites tested with an automated attack tool

18

sites carrying a critical-CVSS attack

51%

(53 of 103) vulnerable to ≥ 1 high-severity flaw

Key finding

Implementation flaws at the relying-party (website) level — not the FIDO2 protocol itself — remain the real residual risk. Attacks in this study could hijack accounts, delete a victim's passkeys, or lock them out entirely.

Separately: *account recovery after a lost device still often falls back to weaker methods (SMS codes, email links) — reintroducing phishing risk at the recovery step.*

Sources: Jannett et al., USENIX Security '26 [8]; Blessing et al., PoPETs 2025 [9]

SECTION 5

Three Influential Organizations

1

FIDO Alliance

INDUSTRY CONSORTIUM

Google, Apple, Microsoft, Amazon, banks, and others. Defines the FIDO2/CTAP2 specifications underlying passkeys and publishes the annual State of Passkeys adoption research.

2

NIST

U.S. FEDERAL STANDARDS AGENCY

SP 800-63 Digital Identity Guidelines define authenticator assurance levels. As of SP 800-63B-4 (2025), phishing-resistant authentication is formally required for high-assurance federal systems.

3

W3C Web Authentication Working Group

STANDARDS BODY

Maintains the WebAuthn API — the browser-facing protocol letting websites request and verify passkey logins — in coordination with the FIDO Alliance's CTAP2.

Three Most Important Sources

[8] L. Jannett et al., “The State of Passkeys: Studying the Adoption and Security of Passkeys on the Web,” Proc. 35th USENIX Security Symposium, 2026, pp. 5039–5058.

[9] J. Blessing, D. Hugenroth, R. Anderson, A. Beresford, “SoK: Web Authentication and Recovery in the Age of End-to-End Encryption,” Proc. Privacy Enhancing Technologies, vol. 2025, no. 3, pp. 560–589.

[5] National Institute of Standards and Technology, “Digital Identity Guidelines: Authentication and Authenticator Management,” NIST SP 800-63B-4, U.S. Dept. of Commerce, 2025.

Selected as independent, technically rigorous, and non-promotional — [8], [9] are peer-reviewed academic security papers; [5] is a binding U.S. federal standard. FIDO Alliance [1] is used only for adoption statistics, as this report's one permitted industry reference.

Conclusion

- Passkeys structurally close phishing and credential-stuffing risk via origin-bound key pairs.
- Password managers still concentrate risk behind one master password — the 2022 LastPass breach shows the real-world cost.
- The two are converging, but residual risk now sits at the relying-party implementation level, not the FIDO2 protocol.